CO-EXISTENCE OF WIRELESS COMMUNICATION SYSTEMS IN ISM BANDS: AN ANALYTICAL STUDY

WANG FENG

(B.Eng)

A THESIS SUBMITTED

FOR THE DEGREE OF DOCTOR OF PHILOSOPHY IN ELECTRICAL ENGINEERING

DEPARTMENT OF ELECTRICAL & COMPUTER ENGINEERING

NATIONAL UNIVERSITY OF SINGAPORE

2004

ACKNOWLEDGEMENTS

This thesis would not have been completed without the help of many people. I would first like to express my heartfelt gratitude to my supervisor, Dr. Nallanathan Arumugam, for his valuable guidance and advice during different phases of my research, especially for his effect on my serious-minded research attitude. I would also like to thank Associate Professor Garg Hari Krishna for offering me the opportunity to study in NUS and his encouragement for me to take the challenges. In addition, I need thank to NUS and ECE-I^2R laboratory for giving me the scholarship and providing a wonderful technical environment. I am also grateful to all my friends for their friendship and great time we spent together. Last but not least, I deeply appreciate my family for their selfless and substantial support. Firstly thanks to my husband, for his endless love, patient and encouragement throughout my Ph.D. studying period. Secondly thanks to my son. His birth brought me a new life and new angle of view to look at this world. And last to my parents, thanks them for sharing my burden in taking care of my new born baby, and their encouragement for me to conquer various difficulties.

TABLE OF CONTENTS

SUMMARY

This thesis studies the mutual interference between the Bluetooth and IEEE 802.11 network, and proposes a scheme to enhance the systems' performance by selecting appropriate parameters, such as packet type, packet segmentation size, adaptive data rate, transmit distance, etc., consequently to allow the two systems to operate in a shared environment without significantly impacting the performance of each other.

The analysis comprises interference at the physical (PHY) and the medium access control (MAC) layers of both systems. At the PHY layer the key calculation is bit error probability. The research includes performance of specific modulations for the Bluetooth receiver and the various IEEE 802.11b data rates. The frequency hopping and direct sequence spread spectrum technologies employed in the two systems are introduced as well as the new proposed complementary code keying (CCK) modulation. Bit error probability as a function of E_b/N_0 is derived for CCK based on the Intersil HFA3861 Rake receiver.

At the MAC layer, collision probability for the Bluetooth or 802.11 packet overlapped by interfering packets in both time and frequency is thoroughly analyzed. All of collision scenarios are considered, which are Bluetooth collided by Bluetooth, Bluetooth collided by 802.11b, and 802.11b collided by Bluetooth. In addition all Bluetooth packet types are taken into account. The collision probability obtained at last is a general expression which could be used to compute for any length of the packet, any length of the interval between two packets, and any length of the interfering packet. Results show that there are different numbers of co-worked competitors that a Bluetooth piconet can tolerate at each packet type it used. Considering fairness among all the piconets, the same packet type should be used in each piconet. We find 1-slot packet type is suitable for high density interference

environment; 3-slot type suits the moderate density environment; while 5-slot type is used when there are few piconets. In the mixed environment of Bluetooth and 802.11b, Bluetooth should use the packet type of 5-slot time long to reduce its hop rate, thereby increasing the chances of successful reception of WLAN packets.

When considering the system performance, Packet Error Rate (PER) is used as the metric parameter. The analysis of PER consists of both PHY and MAC layers. We develop a model for the analysis of PER by means of an integrated approach, which properly takes into account all transmission aspects (propagation distance, interference, thermal noise, modulations, data rates, packet size). Thus system performance over a distance is obtained.

By using the proposed evaluation framework, the optimum packet type, segmentation size, safe distance ratio and data rate for the transmitter and receiver at current link condition are easily obtained. We find the safe distance ratio for an 802.11b receiver to the Bluetooth interference. Thus when the WLAN is operating in safe distance or interference free environment, the long segmentation size of 2350 bytes is suggested to use. Then the optimum packet sizes are found for each data rate under significant interference from Bluetooth. The proper moment for data rate scaling of the system is found that 11 Mbps has the maximum throughput in the presence of one Bluetooth piconet. When piconets increase, 11 Mbps mode has to be abandoned, and data rate scaling can take place in the proper distance ratio.

NOMENCLATURE

ACL	Asynchronous ConnectionLess
AFH	adaptive frequency hopping
ARQ	automatic repeat request
AWGN	additive white Gaussian noise
BER	bit error rate
BSS	basic service set
CCA	clear channel assessment
CCK	complementary code keying
CPFSK	continuous phase frequency shift keying
CRC	cyclic redundancy check
CSMA/CA	carrier-sense, multiple accesses, collision avoidance
CTS	clear-to-send
CW	contention window
DBPSK	differential binary phase shift keying
DCF	distributed coordination function
DIFS	DCF interframe space
DQPSK	differential quadrature phase shift keying
DSSS	direct sequence spread spectrum
FEC	forward error correction
FHSS	frequency hopping spread spectrum
FSK	frequency shift keying
FWT	fast walsh transform
GFSK	Gaussian frequency shift keying
ISI	inter-symbol interference

ISM	industrial, scientific, and medical
LBT	listen-before-talk
LOS	line-of-sight
MAC	medium access control
NAV	network allocation vector
OBS	obstructed direct path
PCF	point coordination function
PDF	probability density function
PER	packet error rate
PHY	physical
PLCP	physical Layer convergence protocol
RTS	request-to-send
SCO	Synchronous Connection-Oriented
SIFS	short interframe space
SIG	special interest group
SIR	signal-to-interference ratio
SINR	signal-to-noise-interference ratio
SNR	signal-to-noise ratio
TDD	time division duplex
WLAN	wireless local area network
WPAN	wireless personal area network

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Background

Wireless communication networks are getting more and more popular in the networking era. Wireless computing technology provides users with network connectivity without wired connection. According to the communication distance between the transmitter and the receiver, we can classify the wireless network standards into Wide Area Network (WAN), Wireless Local Area Network (WLAN) and Wireless Personal Area Network (WPAN), as is shown in Figure 1.1. These three types of wireless networks establish a ubiquitous wireless communications for people at anytime anywhere.

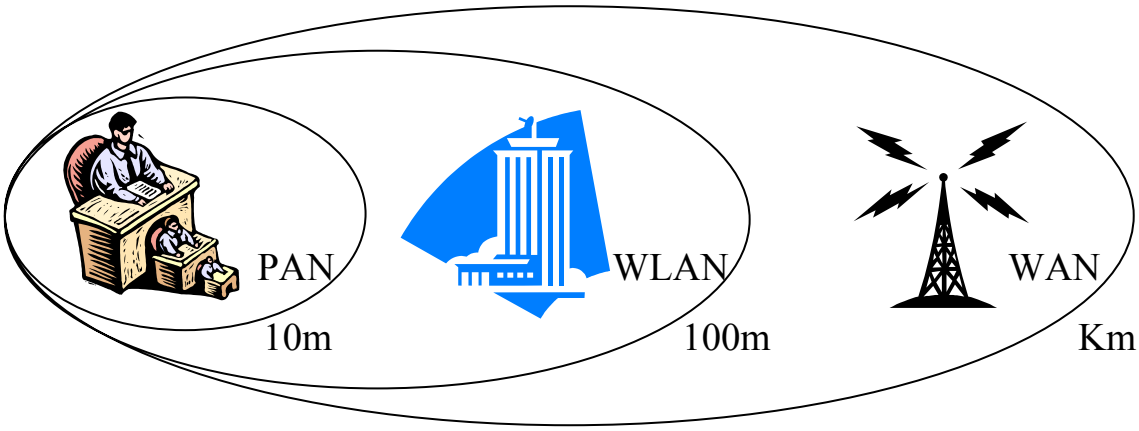

Figure 1.1 A ubiquitous wireless networking structure

WANs provide a large range (up to several kilometers) of communication applications, such as vehicular phone, personal handphone, position sensing, etc. WLANs, like their wired counterparts, are being developed to provide high bandwidth to users in a

limited geographical area. With WLANs, applications such as Internet access, e-mail and file sharing can now be done in the home or office environments with new levels of freedom and flexibility. At the same time, WPANs led by a short-range wireless technology called Bluetooth is created to fulfill a desire of wireless connection of portable devices. Current portable devices use infrared links to communicate with each other. They have a limited range, require direct line-of-sight, are sensitive to direction, and can only be used between two devices. In contrast, Bluetooth can have much greater range (defined to 10 meters), can propagate around objects and through various materials, and connect to many devices simultaneously. Bluetooth is designed principally for cable replacement applications. Bluetooth is ideal for applications such as wireless headsets, wireless synchronization of PDAs with computers, and wireless peripherals such as printers or keyboards. WLAN and WPAN categories have several technologies competing for dominance; however, based on current market momentum, it appears that IEEE 802.11 and Bluetooth are prevailing.

To operate worldwide, both IEEE 802.11 and Bluetooth select to operate in the 2.4 GHz Industrial, Scientific, and Medical (ISM) band that satisfies such requirements, which ranges from 2,400 to 2,483.5 MHz in the United States and Europe. The 2.4 GHz ISM band is practically attractive because it enjoys worldwide allocations for unlicensed operation, as summarized in Table 1.1.

Table 1.1 Global Spectrum Allocation at 2.4 GHz

Region	**Allocated Spectrum**
US	2.4000-2.4835 GHz
Europe	2.4000-2.4835 GHz
Japan	2.4710-2.4970 GHz
France	2.4465-2.4835 GHz
Spain	2.4450-2.4750 GHz

Because both technologies occupy the 2.4 GHz frequency band, there is potential for interference between the two technologies. However, WPAN and WLAN are complementary rather than competing technologies, and many application models have been envisioned for situations requiring Bluetooth and 802.11 to operate simultaneously and in close proximity. For example, there are many devices, such as laptops, that might use Bluetooth for connection to peripheral devices and 802.11b for network access by equipping both networking components. Thus problem of coexistence between these technologies has become a significant topic of analysis and discussion throughout the industry. Moreover, with both of them expecting rapid growth, physically closed location of the WLAN and WPAN devices will become increasingly likely.

Consequently, the emphasis of the work presented in this thesis is on the analysis of the mutual interference between IEEE 802.11 and Bluetooth at both physical layer and medium access control layer in close proximity environment. Furthermore, non-collaborative solutions on enhancing both systems' performance are proposed as well through changing the parameters of such as packet type, packet size, data rate, distance between the transmitter and the receiver, and etc.

1.2 Problem Statement

With high expectations for Bluetooth and 802.11 in the near future, the mutual interference between them has attracted much attention in the industry and academia area. In order to mitigate interference between the two wireless systems, IEEE 802.15 (similar standard as Bluetooth) Working Group has created the Task Group 2 (TG2), which is devoted to the development of coexistence mechanisms [70]; and the

Bluetooth Special Interest Group (SIG) has created a Coexistence Working Group, which focuses on the coexistence problem too. Before appropriate schemes can be proposed, it is necessary to study system performance as defined in the standards and specifications thoroughly. Such a study includes performance of a specific modulation, error correction capability of the receiver, signal propagation environment, system interference immunity, etc. The simplest understanding of the effect of interference is that the receiver cannot distinguish between noise and signal and thus makes an erroneous decision. Both systems have defined Physical (PHY) and Medium Access Control (MAC) layers. The error viewed from the PHY layer is caused by noise (colored or white) added into the information signal. Generally, a metric used in evaluating the performance in the PHY layer is the Bit Error Rate (BER), which depends on the signal-to-noise ratio (SNR). Signal energy is affected by signal attenuation along the propagation path and envelope and phase fluctuations with environment. The error viewed from the MAC layer is caused by interference jumping to the signal's channel during transmission time. The metric used in evaluating the performance in the MAC layer is collision probability. System performances are evaluated through Packet Error Rate (PER) and data throughput, where the results are based on detailed models for the PHY and MAC layers, interference distribution, and wireless channel for signal propagation.

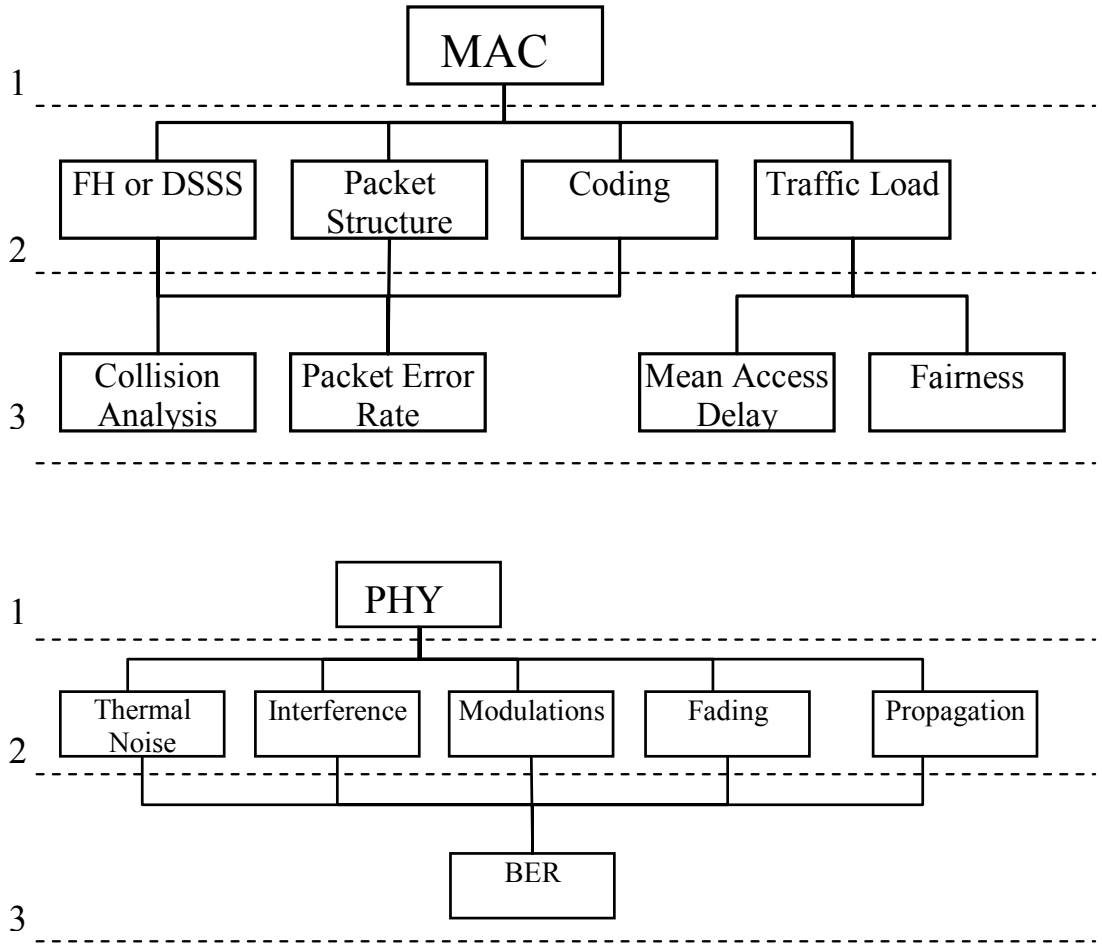

Figure 1.2 Block diagram of the contents in my research topic

As shown in Figure 1.2, there are some properties considered under each layer, which we use to analyze the system performance. The specifications of Bluetooth and 802.11 WLAN define frequency hopping (FH) and direct sequence spread spectrum (DSSS) communication system at the MAC layer. The two spread spectrum systems affect the collision probability of transmitted packets of Bluetooth and 802.11 WLAN. Bluetooth defines 79 hopping channels and jumps from one frequency to another at the end of each packet transmission. On the other hand, 802.11 system uses a channel as wide as 22 MHz which may easily be occupied by Bluetooth packets. Bits in a packet are protected by different coding schemes depending on the different functional parts

in the packet structure. Coding combined with packet structure affect the packet error rate of the system. Some additional (secondary) performance metrics at the MAC layer include the mean access delay and the fairness of access among users [89]. The access delay measures the time it takes to transmit a packet from the time it is passed to the MAC layer until it is successfully received at the destination. If packets are transmitted at bad frequencies, the retransmission of these lost packets expends more time and increase the mean access delay. The basic idea in fairness algorithms is for sources experiencing a bad wireless link to relinquish the unutilized bandwidth to other sources that can take advantage of it. To compensate their utilization in bandwidth, those sources can re-seize the bandwidth when channel conditions improve. Thus the so-called long term fairness objective is achieved. In the PHY layer, the transmitted signal through the channel is corrupted by the addition of noise and interference, or is distorted through a fading multipath channel. An appropriate modulation scheme and data rate could mitigate those effects to a tolerable level. An accurate computation of the BER would take into consideration factors such as thermal noise, interference, modulation type, channel fading and signal propagation patterns. Performance analysis such as computing BER or PER just gives us an insight of how different systems work in a particular scenario, but not tell how they could work together. Given the importance of the coexistence of Bluetooth and 802.11, there has been considerable research on this topic. Most methods concentrate on changing some behavior in the MAC layer, such as by rescheduling packets or otherwise altering traffic. Such approaches are categorized into collaborative and non-collaborative schemes. Collaborative schemes require a co-located Bluetooth and 802.11b receiver in the same terminal, thus making them possible to exchange information to reduce mutual interference. With non-collaborative schemes, there is no way for

heterogeneous systems to exchange information between the two network systems, and they operate independently.

In this thesis we try to propose a scheme by selecting appropriate parameters, such as packet structure, information length, adaptive data speed, transmit distance and etc., consequently allow the two systems can operate in a shared environment without significantly impacting the performance of each other. This scheme does not need any change in the current IEEE 802.11 and Bluetooth MAC protocol.

1.3 Related Work

The coexistence issue has been investigated separately considering the impact of one system on the other. Based on different FH code patterns, several Bluetooth piconets can coexist in the same area. Without coordination among piconets, transmissions from different piconets will inevitably encounter the collision problem. Collision analysis of a Bluetooth in the presence of other piconets was addressed in [1-5]. Zurbes *el al.* [1] presented simulation results for a number of Blueooth devices located in a single large room. They showed that for 100 concurrent web sessions, performance was degraded by only five percent. They also found using long uncoded packet type could improve system throughput. In [2], Souissi analyzed adjacent channel interference as well as co-channel interference. It was concluded that as the number of picoents increased, adjacent channel interference impacted throughput approximately with the same severity as co-channel interference. El-Hoiydi [3] investigated the co-channel interference between Bluetooth piconets and derives collision probability for an interfered Blueooth. But the analysis in [3] had two limitations. First, all packets were assumed to be single-slot ones. Secondly, it was

assumed that each piconet was fully loaded. These constraints were remedied in paper [5]. In [5], a more general analysis model with all packet types (1-, 3- and 5-slot) was proposed, and the model allowed the performance analysis not necessarily based on fully-loaded assumption. On the other hand, capture effects were considered in [4]. Capture effects due to the dependency of the interference level on the spatial distribution of terminals and on the characteristics of the environment make the throughput inhomogeneous over the area. The results showed that when the dimensions of the area were comparable with the coverage area of the terminal, capture effects were practically negligible so that packet error probability was in good agreement with the packet collision probability obtained in [3]. Instead, if the area dimensions were larger than the terminal coverage area, the packet error probability could significantly change with the receiver position.

Few literatures had addressed mutual interference among 802.11b stations. It is because the assumption of that 802.11b stations can determine if the channel is occupied by other 802.11b transmitters is usually used, which based on the default scheme known as Carrier-Sense, Multiple Access, Collision Avoidance (CSMA/CA) used in 802.11b MAC protocol operation. Therefore the analysis and discussion on collision among 802.11b stations is ignored.

Golmie and Mouveaux [6] studied the effect of 802.11 on Bluetooth using an analytical approach, and validated the analysis with simulation results. They showed that significant packet loss can occur and that access delays for data traffic will double. Moreover, the number of residual errors in accepted voice packets could be quite high. Similar results had been obtained by Lansford *et al.* [7] who used simulation and experimental measurements to quantify the interference resulting from Bluetooth and 802.11. Their simulation models were based on a link budget analysis and a Q

function calculation for the channel and PHY models respectively, in addition to the MAC layer behavior. Howitt [8] developed a new methodology to evaluate the impact of an 802.11b network on the Bluetooth performance. The packet collision probability was estimated based on extensive trials for each considered scenario. The empirical results provided an estimate of the likelihood which may cause a collision at a given carrier frequency offset, f_{offset}. As far as the reciprocal scenario is concerned, different studies have been presented about the effect of Bluetooth impact on IEEE 802.11. The probability of an 802.11 packet error in the presence of a Bluetooth piconet had been derived by Ennis [9], then extended by Zyren [10] and Shellhammer [11]. The investigation focused on the probability computation for a continuous sequence of Bluetooth packets overlapping on an 802.11b packet in both time and frequency. However, the analysis presented in [9-11] is based on coarse assumptions and the proposed interference models were not suitable for a thorough study of the system dynamics. Thus in [12], an accurate and flexible model was developed to evaluate the packet error probability of an 802.11 in the presence of either a voice or a data Bluetooth link. The model based on the assumption that a Bluetooth piconet won't transmit in sense of back-to-back mode, consequently, a simple traffic shaping mechanism is used to Bluetooth data flow and a significant reduction of the WLAN packet error probability was observed. Howitt [13, 14] investigated the effect of Bluetooth on 802.11 in another angle. He presented a method on how to determine the expected number of Bluetooth piconets that have sufficient power to cause interference to an 802.11b station. But his method was heavily tied to geometric distribution of Bluetooth piconets which may not be available in a realistic situation.

However, the above literatures did not consider that the destructive effect of packet collisions could be mitigated by the attenuation introduced by the propagation distance.

Thus there have been several attempts at quantifying the impact of interference on both the Bluetooth and IEEE 802.11 performance. The average power of signal and interference received at the receiver is considered to experience large scale fading over a large area as a function of distance. In [15] the issue of the coexistence of Bluetooth piconets deployed in the same region had been addressed; the analytical derivation of packet error rate had been carried out taking propagation aspects into account, moreover the optimal number of piconets which maximize the aggregated throughput has been suggested. Experimental methodology for the voice performance of Bluetooth in the presence of WLAN 802.11 system was proposed in [16]. An OPNET platform was used to build the propagation model and the interference models, then implemented by C language and assisted by Matlab software. But the authors did not give much useful results on this. For the issue of Bluetooth interference on 802.11, experimental measurements were obtained by Kamerman [25]. Zyren [23] studied 802.11 high speed performance in a Bluetooth mixed environment, where propagation model and user traffic loads were considered. Jo [24] extended two-node WLAN system to a multiple 802.11b WLAN stations topology. They obtained results for light and heavy Bluetooth usage scenarios, the 802.11b system throughputs were degraded by 25% and 66% respectively. Fainberg [17] developed a model that captures the performance parameterized by the data rate and packet size of 802.11b, the number of Bluetooth picoents, the piconet utilization, and the distance between the 802.11b and the Bluetooth radios. His calculation in packet error rate was accurate to bit level which takes into account of the number of bits involved in collision and not in collision. The results showed that the effect of Bluetooth radios on the 802.11b system is significant. In a high density of Bluetooth piconets environment, only 11 Mbps data rate with short packet transmission time provided reasonable throughput for a 25-meter

radius area. Golmei [18,19] presented a simulation environment for modeling mutual interference, i.e. Bluetooth versus 802.11 and 802.11 versus Bluetooth, based on detailed MAC and PHY model. Four different simulation experiments that showed the impact of WLAN interference on Bluetooth devices and vice versa for different applications were implemented in the OPNET simulation. The results indicated that Bluetooth voice traffic can cause 65% of packet loss for the WLAN 1 Mbps system. On the converse, Bluetooth voice can be severely affected by 802.11b with packet loss of 8%. Conti *et al.* [20-22], on the other hand, developed an integrated analytical approach that was carefully proposed taking into account both PHY and MAC layer aspects. The mean packet error probability was evaluated as a function of the relative distance between the two systems for different conditions. They simply assumed a simple exponential expression, $P_s = ae^{-b\gamma}$, as the instantaneous symbol error probability and used it for both considered systems; but the error probability of various modulations, corresponding to four data rates, of 802.11b, which affect the system performance very much, were not taken into consideration.

Coexistence issue between Bluetooth and 802.11 is another popular topic lately and addressed in a lot of literatures. According to the IEEE 802.15 Working Group, coexistence of 802.11b and 802.15 occurs when the two systems can operate in a shared environment without significantly impacting the performance of each other [69]. Two classes of coexistence mechanisms have been defined: collaborative and non-collaborative techniques [26]. With collaborative techniques, there is possible control centre for the Bluetooth network and the WLAN to exchange information and schedule their packets transmission time to reduce the collision probability; however, they can be implemented only when the Bluetooth and the 802.11 devices are collocated in the same terminal. With non-collaborative techniques, there is no way to exchange

information between the two systems, and they operate independently. Within the literatures, non-collaborative coexistence mechanisms have attracted more interest because many application models are working independently. This is a more realistic situation that can be found in office or home environment. Non-collaborative coexistence mechanisms include a number of techniques and schemes, such as adaptive frequency hopping (AFH), transmit power control, Listen-Before-Talk (LBT), adaptive packet selection and scheduling, adaptive error correction coding rate, traffic scheduling, and etc. According to the AFH scheme [72][73][74], Bluetooth frequency channels were classified as "good" or "bad" and were used intelligently to reduce the probability of overlap in frequency with the 802.11 signal. In [76], the transmit power control scheme was presented. This power control technique was based on the idea that 802.11 and Bluetooth devices should reduce their transmission power as much as possible to reduce interference. Therefore, under the conditions of guaranteed BER, the transmission power should be as low as possible. The scheme also incorporated with the algorithm of the highest mandatory rate at lower transmit power, i.e., when possible, the 802.11 devices would shift to the highest rate using lower transmit power. A hybrid method of power control, AFH and LBT was proposed in [27]. The results showed that power control mitigated the number of potential interferers, LBT combats interference from other piconets and AFH combats interference from 802.11 efficiently. The effect of separation distance between two systems is evaluated in several literatures. According to the IEEE 802.15 working group, interference between 802.11 and Bluetooth causes a severe degradation of the systems' throughput when the distance between interfering devices is less than 2 m. A slightly less significant degradation is observed when the distance ranges between 2 and 4 m [71]. Experiments conducted in [28] evaluated actual Bluetooth and 802.11b radios with

respect to actual office usage. It was found that it was necessary to keep 802.11b DSSS and Bluetooth radios at least three meters apart. Similar experiments and results were implemented and obtained in [29]. Adaptive packet selection and scheduling [75] could be effectively used to mitigate interference between 802.11 and Bluetooth. By selecting the best Bluetooth packet type according to the condition of the upcoming frequency hop, Bluetooth throughput was improved. Also, Bluetooth transmissions could be scheduled in such a way that hops in the 802.11 band were avoided, thus reducing interference between the two radio systems. In order to achieve the large capacity for Bluetooth data connections, long and uncoded Bluetooth packet types were suggested to use in data transmission [30]. Extensive schemes were proposed to change some behavior of MAC layer. Adaptive data rate scaling algorithm for 802.11 was proposed in [31]. After selecting optimum retransmission limit when designing the algorithm, the algorithm could indicate the 802.11 WLAN to select the best rate for a particular frame transmission. An optimum retransmission limit was observed. Valenti [32] explored a custom Forward-Error-Correction (FEC) coding which was different from the Hamming codes used by Bluetooth data packets. The selected coding was BCH code and its code rate was adaptive to match the channel conditions. Chiasserini [33] proposed two novel coexistence schemes, called overlap avoidance (OLA), which were based on simple traffic scheduling techniques. Voice-OLA was used to avoid overlap in time between the Bluetooth SCO traffic and the 802.11 packets. Data-OLA was to use the variety of packet lengths that characterize the Bluetooth system to avoid overlap in frequency between 802.11 and Bluetooth transmission. The results showed that by applying the voice-OLA, system throughput improved 10%. The improvement achieved by using the data-OLA improved to 50% for Bluetooth heavy traffic load. Traffic adaptive retransmission scheme is proposed

in [34]. Its principle is by controlling the number of retransmission packets to reduce the serious contention for the heavy traffic loaded channel. The results show that the real-time traffic could be rapidly transmitted without the effects of large delay. Other measurements such as the issue of receiver improvement were considered in [35] and [36]. Solution for higher layer such as networking layer was proposed in [37]. Several scheduling algorithms were proposed based on queuing priority policy providing fairness to access the shared channel.

1.4 Thesis Contribution

The aim of this thesis is to perform a complete analytical study on mutual interference and performance enhancement of two systems by means of an integrated approach, which properly takes all transmission aspects (propagation effects, interference, thermal noise, modulations, coding techniques, data rates) and medium access control aspects (frequency hopping, packet type, packet size adjustment, traffic load) into account. Though we are not the first to propose an integrated approach to study the coexistence problem in a complete theoretical analysis, our model is different from others in implementation and complexity. Moreover our model is clearer and more flexible, and can be easily implemented to get numerical results, avoiding the need of extensive bit level Monte Carlo simulations at the PHY level.

This thesis starts with BER analysis in the PHY layer. Modulation schemes such as GFSK used in Bluetooth and DBPSK and DQPSK used in 802.11b are well known and related bit error probability calculation formulas have been given in [38-40] and [41] respectively. For Complementary Code Keying (CCK) modulation however, it was just proposed by Harris Semiconductor and Lucent Technologies in recent years

as extension to 802.11b for higher data rates. To our knowledge, there is no existing formula for the bit error probability in terms of E_b / N_0 for CCK modulation. Thus in this thesis, CCK modulation and demodulation technologies are well explained and the probability of error for CCK is carefully derived based on the Intersil HFA3861 Rake receiver. Results show that at the same E_b / N_0 ratio, CCK 11Mbps outperforms CCK 5.5 Mbps, DBPSK and DQPSK. But if transmit power is fixed, the average bit energy will be much lower at higher data rates than at lower data rates. This is why the actual performance of CCK is worse than that at lower rates. Furthermore, CCK modulation does not have spreading gain at higher data rates, thus its ability to combat interference is worse than at lower data rates. Experimental results have also shown that higher rates are desirable for short range operation and fewer interferers.

Though collision probability between the two systems have been extensively evaluated, e.g. [1-14], no one has thoroughly analyzed this problem in following scenarios: (i) Bluetooth packets colliding with Bluetooth packets; (ii) Bluetooth packets colliding with 802.11b packets; and (iii) 802.11b packets colliding with Bluetooth packets. Furthermore, their analysis had limitations due to the assumption that all Bluetooth packets are single-slot ones. Thus in this thesis, we consider all of these collision scenarios, and in addition, collision of Bluetooth packets of different length, such as the desired packet colliding with single-slot Bluetooth packets; the desired packet colliding with 3-slot Bluetooth packets; and the desired packet colliding with 5-slot Bluetooth packets, are computed too. In our analysis, the collision probability is derived from a group of illustrations that enumerate all possible overlappings by interference packets. The collision probability obtained is a general result which could be used to compute the collision probability for any packet length, any time interval

(including whatever length of idle time) between two packets, and any interfering packet length.

When considering the system performance, we use PER as our metric parameter. The analysis of PER consists of both PHY and MAC layers, thus make it accurate to bit level; i.e. PER occurred when the received packet has at least one bit error. We proposed the method to quantify the received signal power, interference power, hence the SNR, in the calculation of BER. It is categorized into the BER affected by Bluetooth/802.11b interference and the BER affected only by AWGN noise. In the PER calculation, BER affected by interference is used to substitute the bit error probability for bits in the portion that is involved in collision; and BER affected by noise is used to substitute the bit error probability for bits in the portion that is not involved in collision. We also propose the method on how to calculate the portion that is involved in collision for different packet types of Bluetooth and 802.11b. Thus an accurate expression for the mean PER is carried out, which is parameterized by propagation distance, estimated average received signal power, and the number of interferers.

However, people usually care about the efficient data rate, i.e. the throughput of a system. Retaining a low BER or PER performance cannot guarantee the maximum throughput of a system. Thus throughput optimization for both systems in the mutual interference environment becomes an important consideration in our research. In this thesis we try to propose a scheme by selecting appropriate parameters, such as packet types, information length, adaptive data speed, transmit distance and etc., consequently allow the two systems can operate in a shared environment without significantly impacting the performance of each other. Its principle is to improve the efficiency of a system by adapting the PHY and MAC behaviors to the current link condition. A joint

analysis of Bluetooth interference on 802.11b and 802.11b interference on Bluetooth is carried out in order to estimate the minimum coexistence distance as a function of the desired quality of service (QoS). On the other hand, serious interference from Bluetooth could cause the WLAN to scale to a lower data rate. But this mechanism used in current 802.11b system increases packet duration, which lead to larger PER, and then lead to yet a further decrease in the data rate. This problem has not been well discussed and solved in literatures. Thus we propose a scheme to solve the data rate scaling problem. In our scheme, optimum packet sizes for each data rate are found in the condition of different interference scenarios. Then we make the adaptive packet size algorithm prior to the data rate scaling algorithm, which means before the system decides to scale the rate down, it should first try to adjust its packet size to obtain the optimal throughput at that link condition. Data rate scaling adaptation occurs when the maximum throughput of a higher rate is less than that of the lower rate. This proposed scheme does not require any change in the current 802.11 and Bluetooth MAC protocol.

In a summary, the two systems' performance depend on several factors, i.e. signal power, path condition, available channels, packet size, the transmitter-receiver distance and interferers' density. The novelty of this thesis lies in the derivation of a completely analytical framework which allows the determination of the optimal throughput as well as the determination of the optimal operating conditions. The model could be easily implemented to get numerical results.

To our knowledge, no analytical study has been presented in literatures by considering all of the above-mentioned aspects.

1.5 Organization of the Thesis

Analysis in the PHY layer is based on the bit level, thus indoor channel model for WLAN and WPAN is reviewed and appropriate assumption of flat slow fading is explained carefully in Chapter 2. Also GFSK modulation used in Bluetooth and DSSS and CCK techniques used in 802.11b are introduced carefully and their performance under AWGN, fading channel, and interference is given in Chapter 2.

Analysis in the MAC layer is focused on calculating the collision probability of a desired packet when it is in danger of overlapping by packets from different systems in time and frequency. Such calculation includes the impact of a Bluetooth from another Bluetooth piconet; the impact of a Bluetooth from another 802.11b network; and the impact of an 802.11b network from a number of Bluetooth piconets. Though interference among 802.11b stations is proposed for discussion too, we ignored this problem since to assume the CSMA/CA scheme could work well; on the other hand we give detailed explanation on CSMA/CA scheme employed in 802.11b. All these contents are arranged in Chapter 3.

In Chapter 4, a more accurate and practical model is proposed to quantify the mutual interference on the two systems, which combines both PHY and MAC layers together, and takes all transmission aspects into account. As have been considered, signal propagation model is based on large scale fading assumption. The path loss exponent is carefully chosen for WLAN and WPAN operating environment. The path of signal power attenuation is classified into line-of-sight (LOS) if it is less than 8 meters and obstructed direct path (OBS) if it is larger than 8 meters. The method on how to model white/colored interference in the form of SNR is explained in Chapter 4. Concepts of co-channel and adjacent channel interference are clarified under the subsection of colored noise. Furthermore, PER is introduced to represent system performance

instead of collision probability. PER is defined in this thesis as at least one bit in the packet received erroneously. A scenario considered in our analysis consists of a number of Bluetooth piconets assumed to be uniformly distributed in a circular region. However, our analysis model is not necessarily based on the deploying of devices as this scenario. Because we have considered interference from multiple piconets environment, this scenario is just easily used to calculate the total interference power from those piconets at the same distance. For a more realistic scenario, the interference need not be distributed at same distance to the receiver. The total interference power can be calculated separately according to each one's actual distance.

As we have analyzed mutual interference between Bluetooth and 802.11b in Chapter 2, 3 and 4, Chapter 5 is given some performance enhancement solutions for the two systems. Those solutions need not change the PHY and MAC layer's specification in the standard. In this chapter, we try to explain non-collaborative solutions for the coexistence problem. Our analysis is based on the fact that parameters can be adjusted, such as packet types, packet segmentation size, data rate scaling, and distance to interferers. Coexistence mechanism is implemented by selecting appropriate values of these parameters.

Finally, conclusions based on the studies of this thesis are given in Chapter 6. Improvement for imperfect assumptions and the numerical results that need further verification by experimental measurements are addressed in the part of future work. The mutual interference induced from other new technologies in the 2.4 GHz ISM band is mentioned and briefly reviewed at the last part of this chapter.

CHAPTER 2

BIT ERROR RATE ANALYSIS IN PHY LAYER

In this chapter, two wireless technologies, i.e. Bluetooth and IEEE 802.11b, will be introduced. Bit Error Rate (BER) is usually used as the performance analysis metric in the physical layer. Noisy signals are demodulated and decoded at the receiver. A receiver is designed according to different modulation techniques, thus to have best corresponding ability of drawing out the modulated signals from noise. So modulations of GFSK, DBPSK, DQPSK and CCK employed in Bluetooth and IEEE 802.11b systems are introduced. Then the performance of these modulations in the two systems is evaluated under AWGN, fading channel and interference following the introduction.

2.1 Indoor Channel Model

In indoor radio communication, the indoor radio channel depends heavily on the type of building (materials, dimensions, etc.) and objects in their path. Generally, transmitted radio signals propagate via multiple paths which differ in amplitude, phase, and delay time. Therefore, the received information signal is distorted by time dispersion and amplitude fading. Radio propagation measurements include analysis of channel parameters, namely, delay spread τ_{rms} and coherence bandwidth, Doppler spread and coherence time. Delay spread and coherence bandwidth are parameters that describe the time dispersive nature of the channel in a local area. The distance traveled

by the arriving signals are different, i.e., the signals will arrive at the receiver at different time. The difference in time between the earliest and the latest reflection to arrive at the receiver is defined as the delay spread. The coherence bandwidth B_{coh}, is the statistical average bandwidth of the radio channel, over which signal propagation characteristics are correlated. This parameter specifies the frequency range over which a transmission channel affects the signal spectrum nearly in the same way, giving an approximately constant attenuation and a linear change in phase. B_{coh} and τ_{rms} are related by $B_{coh} = 1/\alpha\tau_{rms}$, where α is a constant. The delay spread τ_{rms} has been determined for different types of rooms in [42]. In different situations, the mean values of τ_{rms} at 2.4 GHz range from 10-20 ns according to [42]. Similar studies have been done in [43-45]. The experiments in [45] showed that the root-mean-square (rms) average of the delay spread (τ_{rms}) varied around 30 ns in a typical indoor environment. In another study [43], it was found that the τ_{rms} values were typically less than 75 ns in the lightly obstructed path and 90 ns in the heavily obstructed path. More experiment by [44] reported that an rms delay spread was less than 50 ns normally, but could be as long as 217 ns in a worst case. The mean values of α for line-of-sight (LOS) and obstructed direct path (OBS) are about four and five respectively, which correspond to the coherent bandwidth of about 25 and 20 MHz respectively. Doppler spread and coherence time are parameters that describe the time varying nature of the channel in a small-scale region. When there is relative motion between the transmitter and receiver, the frequency in the received signal spectrum is changed, i.e., Doppler shift. Doppler shift changes from positive to negative when the mobile move towards, then away from the signal source. Coherence time is a statistical measure of the time duration over which two received signals have a strong potential for amplitude correlation.

However, stationary transmitters and receivers are assumed in this thesis, consequently Doppler spread fading is ignored in our analysis. Bluetooth signals are transmitted in a carrier channel of 1 MHz bandwidth; while 802.11b signals are transmitted in a channel about of 22 MHz. As the bandwidths used by both systems are less than the coherent bandwidth in an indoor environment, we chose a flat quasi-static fading channel model, in which the received signal only has amplitude fluctuations due to the variations in the channel gain over time caused by multipath. Moreover, the spectral characteristics of the transmitted signal are assumed to remain intact at the receiver. With quasi-static fading, the envelope of the signal associated with the entire packet is multiplied by the same channel gain which is typically Rayleigh or Rician distributed.

For a LOS path, the power spectral density of the faded amplitude is close to a Rician distribution with $K = 5$ [43], where K is the ratio of the dominant signal to the standard deviation of other weaker and randomly varying signals. At sites with obstacles the measured distribution seems to follow the Rayleigh distribution.

We derive a general result concerning the mean (averaged over Rice/Rayleigh fading) error probability evaluation for an arbitrary modulation scheme. Let the fading signal envelope of the received signal be R. Then the Probability Density Function (PDF) of R can be found by a transformation of variables. The PDF of R in Rayleigh distribution is given as [65]

$$f(R) = \frac{R}{\sigma^2} \exp\left(-\frac{R^2}{2\sigma^2} \right) \tag{2-1}$$

where σ^2 is the time-average power of the received signal before envelope detection.

The PDF of R in Rician distribution is given as

$$f(R) = \frac{R}{\sigma^2} \exp\left(-\frac{R^2 + K^2}{2\sigma^2} \right) I_0\left(\frac{RK}{\sigma^2} \right) \tag{2-2}$$

where σ^2 is as defined above, $I_0(.)$ is the modified Bessel function of the first order and K is the Rice factor.

The fundamental parameter in the BER performance of any modulation scheme is the ratio of energy per bit to noise spectral density, or E_b / N_0. Now in fading channel, as the attenuation R is a random variable, E_b / N_0 must be averaged over its PDF. Then the instantaneous ratio of E_b / N_0 is $\gamma = \frac{R^2 E_b}{N_0}$. The PDF of γ can be found by a transformation of variables. γ is characterized by the following PDF [46]

$$p_\gamma(\gamma) = \frac{(1+K)}{\overline{\gamma}} \exp\left\{-K - \frac{(1+K)\gamma}{\overline{\gamma}}\right\} I_0\left[2\sqrt{\frac{K(1+K)\gamma}{\overline{\gamma}}}\right], \quad \text{for } \gamma \geq 0 \qquad (2\text{-}3)$$

where $\overline{\gamma} = E_b / N_0$ is the mean SNR, $I_0(.)$ is the modified Bessel function of the first order and K is the Rice factor. For LOS, K is between 3 and 10. For obstacles in the path between transmitter and receiver, $K = 0$ reduces to the Rayleigh distribution. The mean bit error rate averaged over the fading density function is $\overline{P}_e = \int_0^\infty P_e(\gamma) \cdot p_\gamma(\gamma) d\gamma$, where $P_e(\gamma)$ is the probability of error for an arbitrary modulation at an instantaneous value of signal to noise ratio (γ) in AWGN channel and $p_\gamma(\gamma)$ is the probability density function of γ due to the fading channel.

2.2 Bluetooth Overview

Bluetooth was developed initially by Ericsson and furthermore by the Bluetooth SIG, which was founded in 1998 to define an industry-wide specification as a short-range (10 meters) cable replacement for linking portable consumer electronic products, but it can also be adapted for printers, fax machines, keyboards, toys, games, and virtually any other digital consumer application. More than a thousand companies are now members of the SIG, signifying the industry's unprecedented acceptance of the Bluetooth wireless technology.

The Bluetooth wireless technology specification provides secure, radiobased transmission of data and voice. It delivers opportunities for rapid, *ad hoc*, automatic, wireless connections, even when devices are not within the line of sight. Bluetooth is a single chip, low-power, wireless communication module. The radio operates in the globally available 2.4GHz ISM band. Bluetooth channels use a Frequency Hopping/Time Division Duplex (FH/TDD) scheme. FH systems divide the frequency band into several hop channels. The FH channel of Bluetooth makes use of equally spaced 79 1-MHz hop channels defined in the 2.4 GHz ISM band. On average, the FH sequence visits each carrier with equal probability. TDD divides the channel into consecutive time slots, each slot lasting $625\,\mu s$; a different hop channel is used for each slot. This gives a highest hop rate of 1600 hops/sec. During a connection, the radio transmitters and receivers are synchronized to hop from one channel to another in a pseudorandom fashion. With Gaussian Frequency Shift Keying (GFSK) modulation, a symbol rate of 1 Mbps is achieved. Two or more units sharing the same channel form a so-called piconet, where one unit acts as a master, controlling the communication in the piconet and the others act as slaves. Figure 2.1 shows the

FH/TDD scheme. Horizontal axis is divided into 625 μs long time slots. Vertical axis is divided in to 79 hop channels. Bluetooth packet is transmitted in different hop channel [47,48].

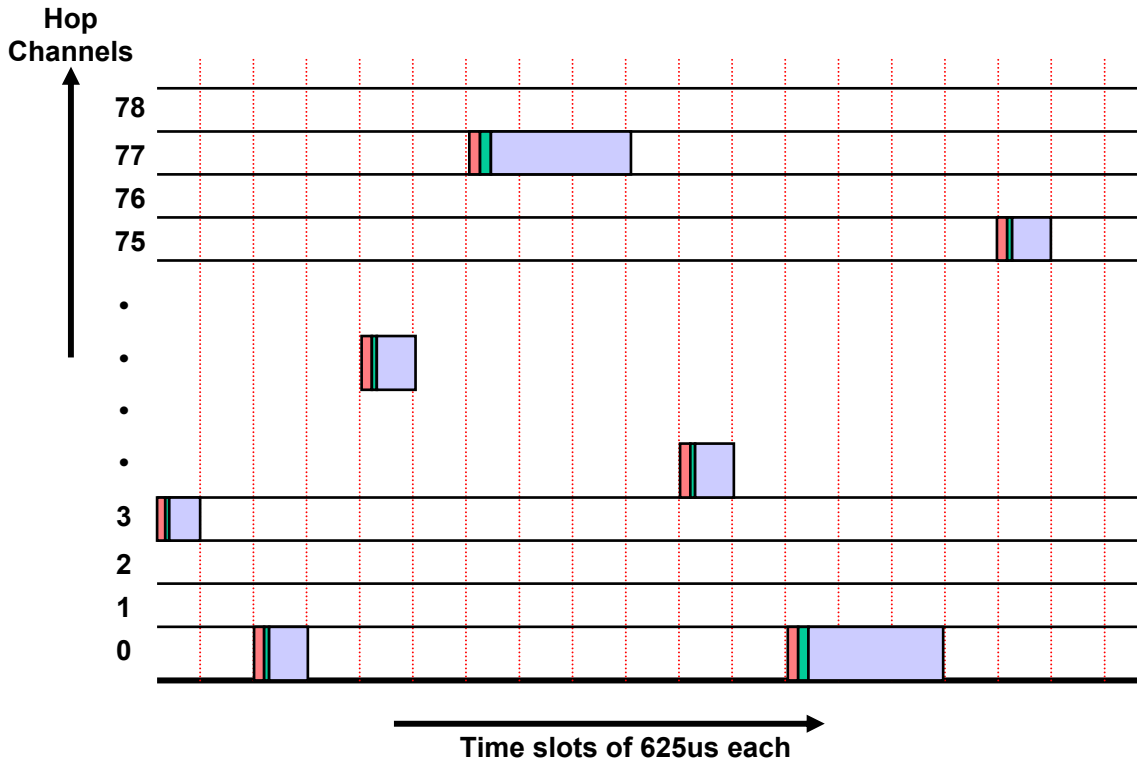

Figure 2.1 Bluetooth FH/TDD scheme

2.3 GFSK Modulation

The modulation chosen in Bluetooth is GFSK with a nominal modulation index h_f between 0.28 and 0.35, and a normalized bandwidth of $B_bT = 0.5$, where B_b is the 3 dB bandwidth of the transmitter's Gaussian low pass filter, and T is the bit period. The modulation index represents the strength of the peak frequency deviation f_d which can be expressed as $f_d = \frac{h_f}{2 \cdot T_b}$, where T_b is the bit duration. This translates to a frequency deviation range of 140 KHz to 175 KHz. The operation of the GFSK modulation can

be better explained after understanding the regular Continuous Phase Frequency Shift Keying (CPFSK). In a memoryless FSK system, abrupt switching from one frequency to another in successive signaling intervals results in relatively large spectral side lobes outside of the main spectral band of the signal and, consequently, this method requires a large frequency band for transmission of the signal. To avoid the use of signals having large spectral side lobes, the information-bearing signal modulates a single carrier in phase whose frequency is changed in a continuous manner. The resulting frequency-modulated signal is phase continuous and hence called CPFSK. This type of FSK signal has memory because the phase of the carrier is constrained to be continuous [49]. A typical sinusoidal wave is described by

$$S(t) = A\cos(\underbrace{2\pi f_c t + \theta(t)}_{\alpha}) \tag{2-4}$$

$$\frac{d\alpha}{dt} = 2\pi f_c + \frac{d\theta(t)}{dt} \tag{2-5}$$

where $A = \sqrt{\frac{2E_b}{T}}$, E_b is the energy per data bit, and f_c is the carrier frequency. $\theta(t)$ is carrying the signal information. $\frac{d\theta(t)}{dt}$ is a variation of frequency. The information is conveyed by phase shifts relative to the previous signal interval. For example, for Minimum Shift Keying (MSK), $\theta(t)$ is given by $\theta(t) = \theta(0) \pm \frac{\pi}{2T}t, \quad 0 \le t \le T$. The information bit 1 is transmitted by shifting the phase of the carrier by $\pi/2$ relative to the previous carrier phase, whereas the information bit 0 is transmitted by a $-\pi/2$ phase shift relative to the phase in the preceding signaling interval.

The transmitted baseband signal is filtered before frequency modulation to further reduce the side lobes. The most popular filters used for this implementation are

Gaussian filters and associated modulation technique is referred to as Gaussian FSK or GFSK. The Gaussian filter smoothes sharp transitions of the voltage levels. As a result we will have a smooth transition from one tone frequency to another that reduces the side lobes of the transmitted signal. As the bandwidth of the filter becomes narrower, the power in the side lobes of the transmitted signal, and consequently adjacent channel interference, reduces. By using GFSK modulation, Bluetooth system can support a raw data rate of 1 Mbps over a 1 MHz channel.

The GFSK signal of Bluetooth can be represented by [50]

$$s(t,a) = A\cos(2\pi f_c t + \phi(t,a)) \tag{2-6}$$

where $A = \sqrt{\frac{2E_b}{T}}$, E_b and f_c are as previously defined. a is the random input stream, comprised of the data bits α_i; $\phi(t,a)$ is the output phase deviation, given by

$$\phi(t,a) = 2\pi h_f \int_{-\infty}^{t} \sum_{i=-\infty}^{n} \alpha_i g(\tau - iT) d\tau \tag{2-7}$$

The Gaussian pulse shaping filter has impulse response $g(t)$ given by

$$g(t) = \frac{1}{2T}\left[Q(2\pi B_b \frac{t - T/2}{\sqrt{\ln 2}}) - Q(2\pi B_b \frac{t + T/2}{\sqrt{\ln 2}}) \right] \tag{2-8}$$

where $Q(t) = \int_t^{\infty} \frac{1}{\sqrt{2\pi}} e^{-x^2/2} dx$ is the standard Q-function. Equation (2-7) can also be written as

$$\phi(t,a) = 2\pi h_f \sum_{i=n-L+1}^{n} \alpha_i q(t - iT) + \pi h_f \sum_{i=-\infty}^{n-L} \alpha_i \tag{2-9}$$

where $q(t) = \int_{-\infty}^{t} g(x) dx$

For Bluetooth with $B_bT = 0.5$, we have $L = 2$, which means that a single data bit is spread over two consecutive symbol intervals. When the signal spread exceeds the bit time of transmission, the energy in the side lobes of the first bit will affect subsequent bits leading to Inter-Symbol Interference (ISI). The impulse response of a Gaussian filter is plotted in Figure 2.2 [51]. It can be found that the curve in Figure 2.2 has sharp edges, which means that the outside lobe introduces less ISI into the modulated signals. Out-of-band energy can usually be filtered out at the receiver, thus the ISI over two consecutive symbols and thus the adjacent channel interference to other systems are ignored.

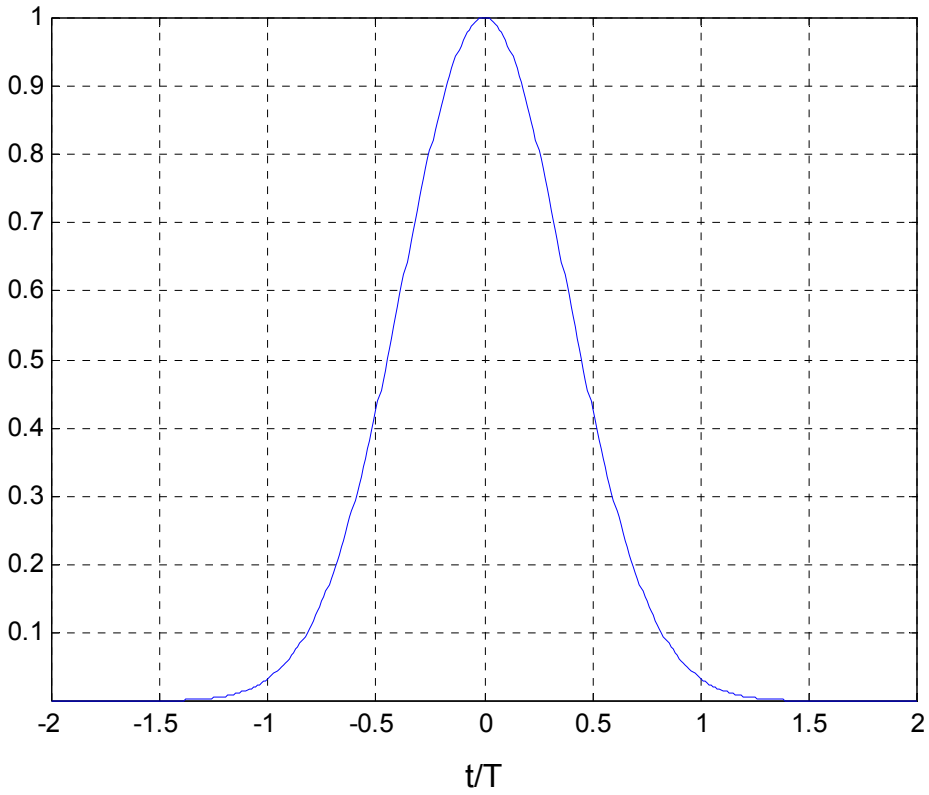

Figure 2.2 Gaussian Pulse

2.4 Performance of Bluetooth

In this section, performance of Bluetooth refers to the performance of Bluetooth GFSK modulation. In [38], a semi-analytical method was presented to obtain Bluetooth's BER performance on an AWGN channel. A more accurate GFSK BER calculation was discussed and obtained in [39]. Recently, in [40], a straightforward and approximate formula was presented. Thus all these methodologies are briefly introduced under this section. Results obtained from these three literatures coincide for low signal to noise ratio.

2.4.1 Under AWGN Channel

2.4.1.1 Semi-analytical Approach

In [38], a semi-analytical approach is used to obtain the overall system performance. A bit level simulation combined with a protocol level simulation was implemented. We briefly introduce some important points. As the error probability is highly dependent on the implementation of the receiver, the proposed receiver model under AWGN noise is shown in Figure 2.3.

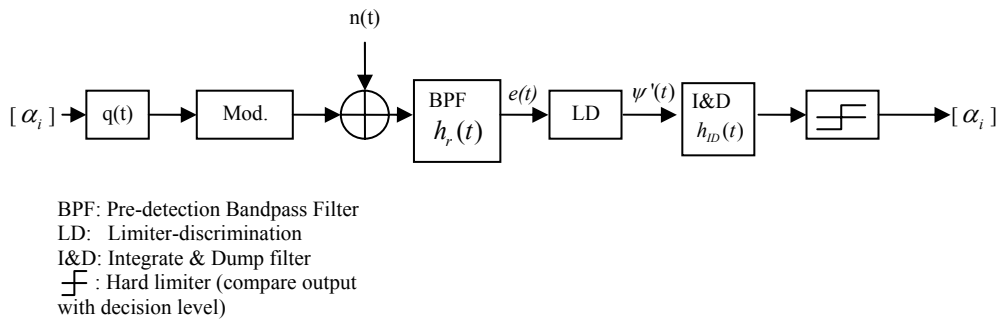

Figure 2.3 Bluetooth system model under AWGN noise

A limiter-discriminator with post-detection integrate and dump filtering (LDI) is used. This receiver consists of a pre-detection bandpass filter (BPF), a limiter-discriminator (LD), and an integrate and dump filter (I&D). The final block is the hard limiter, which compares the output phase with a decision level. The pre-detection bandpass filter is a Gaussian filter with an equivalent lowpass impulse response, $h_r(t)$, given by [52]

$$h_r(t) = \sqrt{\frac{2\pi}{\ln 2}} B_r e^{-\left(\frac{2\pi^2}{\ln 2}\right)\left(B_r t^2\right)} \tag{2-10}$$

where B_r is the 3 dB bandwidth. The optimum bandwidth for this filter is $B_{IF} = 2B_r = 1.1/T$. The discrete impulse response of this filter is obtained by sampling and truncating $h_r(t)$.

The output of the receiver pre-detection filter can be represented using its inphase and quadrature components, $X(t)$ and $Y(t)$, respectively, as

$$\begin{aligned} e(t) &= X(t)\cos(2\pi f_c t) - Y(t)\sin(2\pi f_c t) \\ &= R(t)\cos[2\pi f_c t + \psi(t)] \end{aligned} \tag{2-11}$$

The limiter-discriminator output is thus

$$\psi'(t) = \frac{d\psi(t)}{dt} = \frac{X(t)Y'(t) - X'(t)Y(t)}{X^2(t) + Y^2(t)} \tag{2-12}$$

The discrete impulse response of an ideal differentiator is

$$h_{diff}[n] = \frac{\cos(\pi(n - M/2))}{n - M/2} - \frac{\sin(\pi(n - M/2))}{(n - M/2)^2} \tag{2-13}$$

Truncate this impulse response using a Kaiser window with $M = 5$ and $\beta = 2.4$, and then use it to approximate the derivatives of the quadrature components required in

computing Eq. (2-12). Another approach to implement this filter is to use a simple difference equation.

The integrate-and-dump filter is simply a rectangular filter with impulse response

$$h_{ID}(t) = \begin{cases} 1/T & 0 \le t < T \\ 0 & Otherwise \end{cases} \tag{2-14}$$

The discrete-time filter is obtained by sampling $h_{ID}(t)$. The amplitude of the filter were normalized to 1. The appropriate sampling time for the system is chosen at the maximum eye opening. A simulation is run by generating extensive random signals. To compare the received data via LDI receiver with the original ones, the Bluetooth performance in terms of BER and SNR in the AWGN channel is thus obtained via this model.

2.4.1.2 Accurate Theoretical Approach

In [39], the theoretical BER performance of GFSK is described. They proposed a method for calculating the BER performance of a GFSK system with a post-detection filter and a tank circuit as well as a pre-detection filter, which the system model is shown in Figure 2.4. Tank circuit and the post-detection filter can eliminate the higher harmonics, thermal noise, and interchannel interference from the demodulated baseband signal.

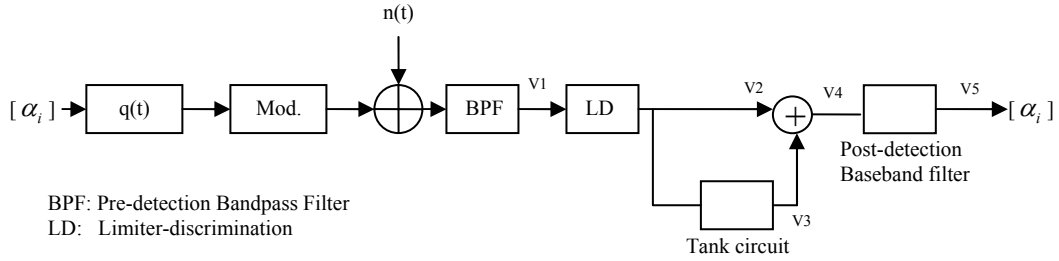

Figure 2.4 System model

A low-pass equivalent expression of the received signal $v_1(t)$ filtered by a pre-detection filter is given by

$$v_1(t) = v_s(t) + n(t) + v_I(t) \tag{2-15}$$

where $v_s(t)$ is the signal of the channel under consideration, $n(t)$ is the additive Gaussian noise, and $v_I(t)$ is the interference signal.

The output signal $v_2(t)$ of the limiter is given by

$$v_2(t) = \frac{4}{\pi}\frac{v_1(t)}{|v_1(t)|} = \frac{4}{\pi}\sqrt{\frac{v_s(t)+n(t)+v_I(t)}{v_s^*(t)+n^*(t)+v_I^*(t)}} \tag{2-16}$$

where * indicates the complex conjugate.

$v_3(t)$ is obtained by convoluting $v_2(t)$ with the impulse response $h_T(t)$, which is

$$\begin{aligned} v_3(t) &= \frac{4}{\pi}\int_{-\infty}^{+\infty} h_T(t)\sqrt{\frac{v_s(t)+n(t)+\delta v_I(t,s)}{v_s^*(t)+n^*(t)+\delta v_I^*(t,s)}}ds \\ &\approx \frac{4}{\pi}\int_{-\infty}^{+\infty} h_T(t)\sqrt{\frac{v_s(t)+n(t)}{v_s^*(t)+n^*(t)}}\cdot\left\{1+j\Im\left[\frac{\delta v_1(t,s)}{v_s(t)+n(t)}\right]\right\}ds \end{aligned} \tag{2-17}$$

Demodulation is carried out by multiplying $v_2(t)$ by the complex conjugate of $v_3(t)$. The resultant output signal $v_4(t)$ is given by

$$v_4(t) = \Re\left[v_2(t)v_3^*(t)\right] \approx \left(\frac{4}{\pi}\right)^2 \Im\left[\int_{-\infty}^{+\infty} \Im\left[h_T(s)\right] \frac{\delta v_2^*(t,s)}{v_s^*(t) + n^*(t)} ds\right] \tag{2-18}$$

The signal $v_4(t)$ is filtered by the post-detection filter and the output signal $v_5(t)$ of the filter is given by

$$\begin{aligned} v_5(t) &= \int_{-\infty}^{+\infty} h_B(u) v_4(t-u) du \\ &\approx \left(\frac{4}{\pi}\right)^2 \Im\left[\int_{-\infty}^{+\infty}\int_{-\infty}^{+\infty} h_B(u) \Im\left[h_T(s)\right] \cdot \frac{\delta v_2^*(t-u,s)}{v_s^*(t-u) + n^*(t-u)} ds du\right] \end{aligned} \tag{2-19}$$

A data decision is made by using the polarity of the output signal $v_5(t)$ of the post-detection filter at sampling time $t = t_0$ with sampling period T. Finally, the average error probability without the interference signal is given by

$$P_e = \frac{1}{N}\sum_{k=1}^{N} P_e^{(k)} \tag{2-20}$$

where $P_e^{(k)}$ is the conditioned error probability for the kth data sequence, which the maximum sequence length needed to account for inter symbol interference is 7 bits. N is the number of possible sequences, which is equal to 128 in the model. Thus GFSK BER performance can be plotted using Eq. (2-20).

2.4.1.3 Approximate Theoretical Approach

However, due to the low cost requirements of Bluetooth, noncoherent receivers are used almost exclusively. A lower bound on error probability can be found by considering the performance of the noncoherent detection of full response binary correlated ($h < 0.5$) FSK signals. This is a lower bound because it does not account

for the additional losses that occur due to ISI induced by the use of partial response GFSK signaling.

A lower bound on Bluetooth GFSK (given the modulation index $h = 0.32$) error probability is given by [40]

$$P_e = Q_1(a,b) - \frac{1}{2}\exp(\frac{a^2+b^2}{2})I_0(ab) \qquad (2\text{-}21)$$

where $Q_1(a,b)$ is the Marcum Q function, $I_0(ab)$ is the modified Bessel function of zero order and parameters *a* and *b* are defined as

$$a = \sqrt{\frac{E_b}{2N_0}(1-\sqrt{1-\rho^2}}$$

$$b = \sqrt{\frac{E_b}{2N_0}(1+\sqrt{1-\rho^2}}\ ,$$

where ρ is the correlation computed in $\rho = \frac{\sin(2\pi h)}{2\pi h}$. It is found that using the results of [39] in place of the performance of full response signaling degrades performance by 5-10 dB, depending on the receiver implementation. Therefore, to obtain a result that can coincide with the results derived by [39] and the Monte Carlo simulation [38], we replace $\frac{E_b}{N_0}$ with $\frac{E_b}{N_0} - 5dB$ in the computation of Eq. (2-21), and then we can get Bluetooth's BER performance in terms of SNR, which is plotted in Figure 2.5. Comparing the results in [38-40], we found they are close fit in the condition of SNR between 0 and 20 dB.

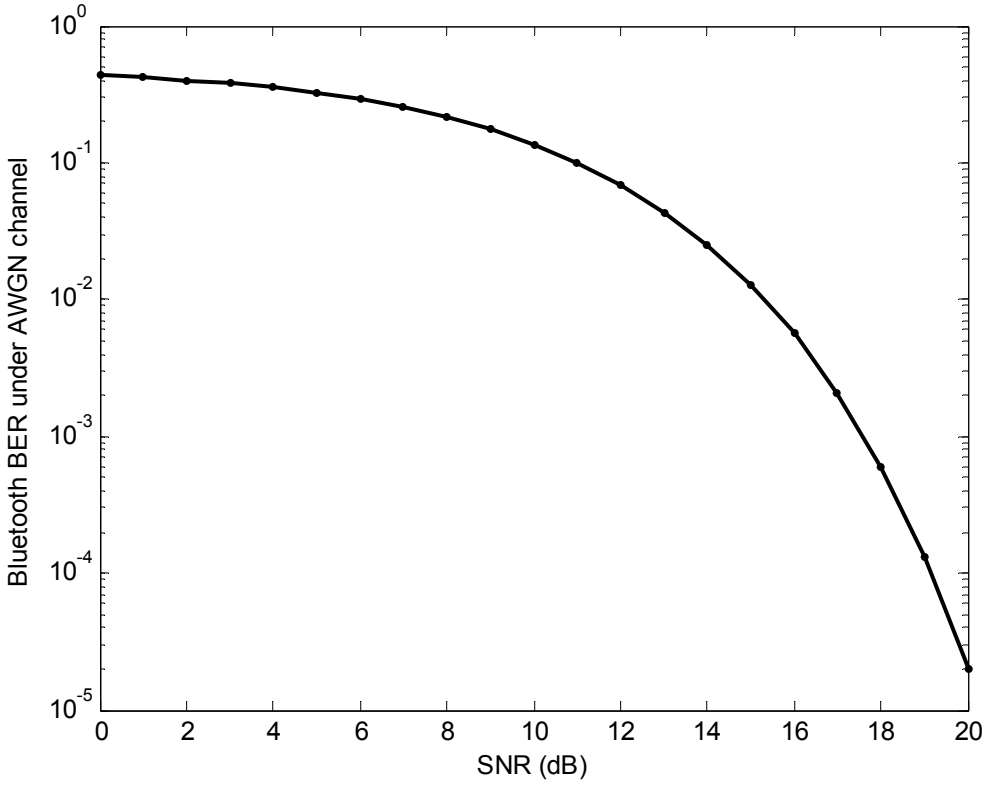

Figure 2.5 Bluetooth BER performance under AWGN channel

2.4.2 Under Fading Channel

Interference is also caused by multipath fading, which is characterized by random amplitude and phase fluctuations of the signal received at the receiver. The reliability of the communications channel is typically measured by the mean bit error rate. For Bluetooth, $P_e(\gamma)$ is the error probability of GFSK modulation at an instantaneous signal to noise ratio γ in the AWGN channel. The mean bit error rate is given by

$$\overline{p_e} = \int_0^\infty \underbrace{\left[Q_1\left(\sqrt{\frac{\gamma}{2}(1-\sqrt{1-\rho^2}}, \sqrt{\frac{\gamma}{2}(1+\sqrt{1-\rho^2}} \right) - \frac{1}{2}\exp(\frac{\gamma}{2}) \cdot I_0(\frac{\gamma\rho}{2}) \right]}_{P_e(\gamma)} \cdot \underbrace{\frac{(1+K)}{\overline{\gamma}} \exp\left\{ -K - \frac{(1+K)\gamma}{\overline{\gamma}} \right\} I_0\left[2\sqrt{\frac{K(1+K)\gamma}{\overline{\gamma}}} \right]}_{P_\gamma(\gamma)} d\gamma \tag{2-22}$$

where $\bar{\gamma}$ is the average SNR.

The performance of Bluetooth in the fading channel as a function of SNR is plotted in Figure 2.6. K is selected as 0, 5 and 10 respectively for Rayleigh, Rician fading.

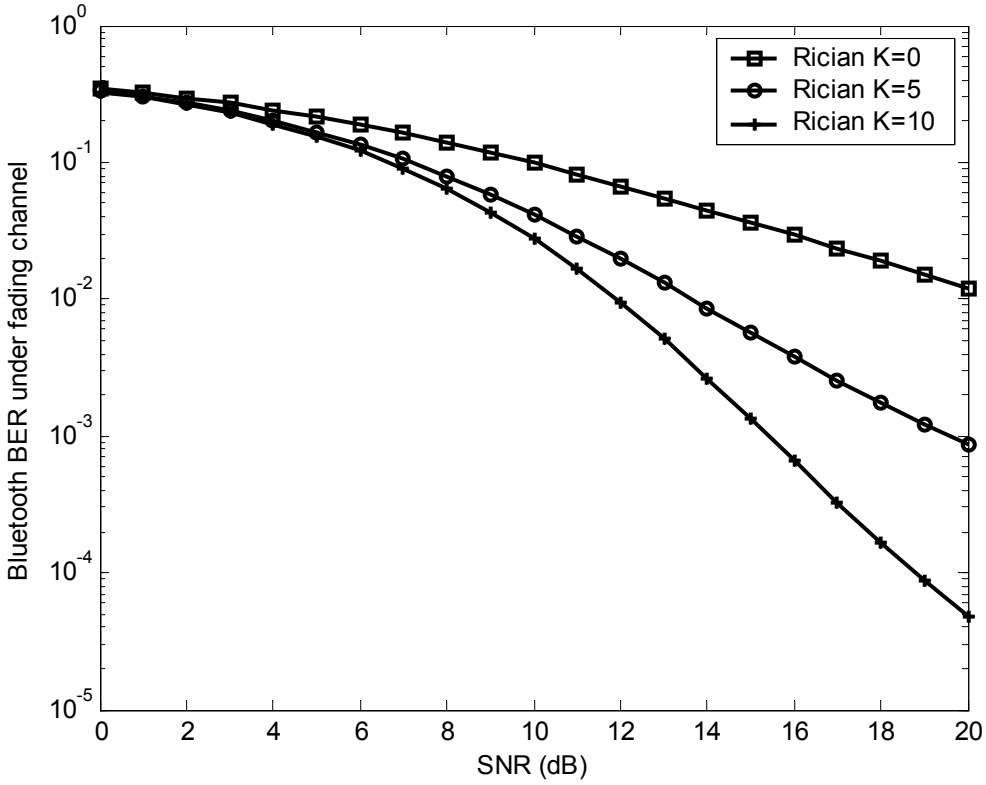

Figure 2.6 Bluetooth BER under fading channels

2.4.3 Under Interference

The frequency hopping (FH) sequence is determined by the master unit in a Bluetooth piconet. The FH patterns for different Bluetooth piconets are uncoordinated, so that multiple piconets operating in the same geographical area will interfere with each other. Two important parameters associated with the receiver are the average signal-to-noise ratio, SNR, and the average signal-to-interference ratio, SIR, defined as

$$SIR = \frac{P_S}{P_I},\ SNR = \frac{P_S}{P_n} \tag{2-23}$$

P_S is the desired signal power; P_I is the interference power, while P_n is the noise power in the receiver's frequency band. The exact distribution for the total co-channel interference is not known. Generally, the interference is approximated as Gaussian [53-55]. The assumption will be well explained in section 4.2. The performance evaluation at the Bluetooth receiver is detected based on the ratio of signal to interference and noise (SINR), which is expressed as $P_S/(P_I + P_n)$. Substituting $\frac{E_b}{N_0}$ with $P_S/(P_I + P_n)$ in Eq. (2-21), we obtained the BER performance of GFSK modulation under interference. Given a certain value of SIR and SNR, the SINR in terms of SIR and SNR is obtained by

$$SINR = \frac{P_S}{P_I + P_n} = \frac{SIR \cdot SNR}{SIR + SNR} \tag{2-24}$$

The co-channel interference will be the dominating source of interference. In Bluetooth, a carrier to co-channel interference ratio $C/I_{co-channel}$ of 11dB is required. The BER performance of a Bluetooth under co-channel interference ratio of 5, 11 and 15 dB is shown in Figure 2.7. Fading is considered as well with interference together. The effect of both of them is shown in Figure 2.8. Thus far, we find the model of [40] is flexible for the performance analysis of Bluetooth in the PHY layer.

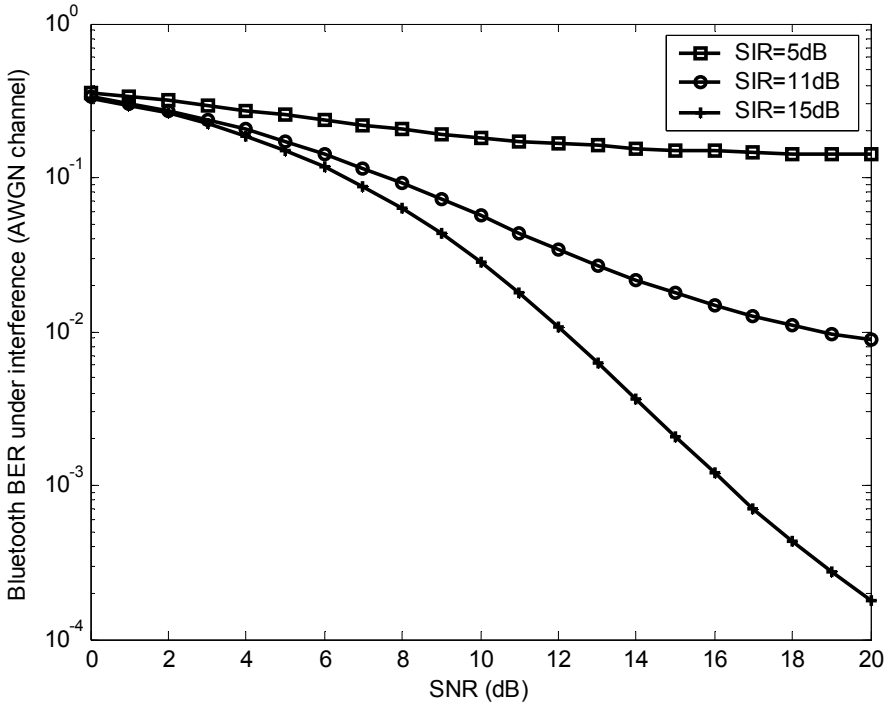

Figure 2.7 Bluetooth BER under interference and AWGN channel

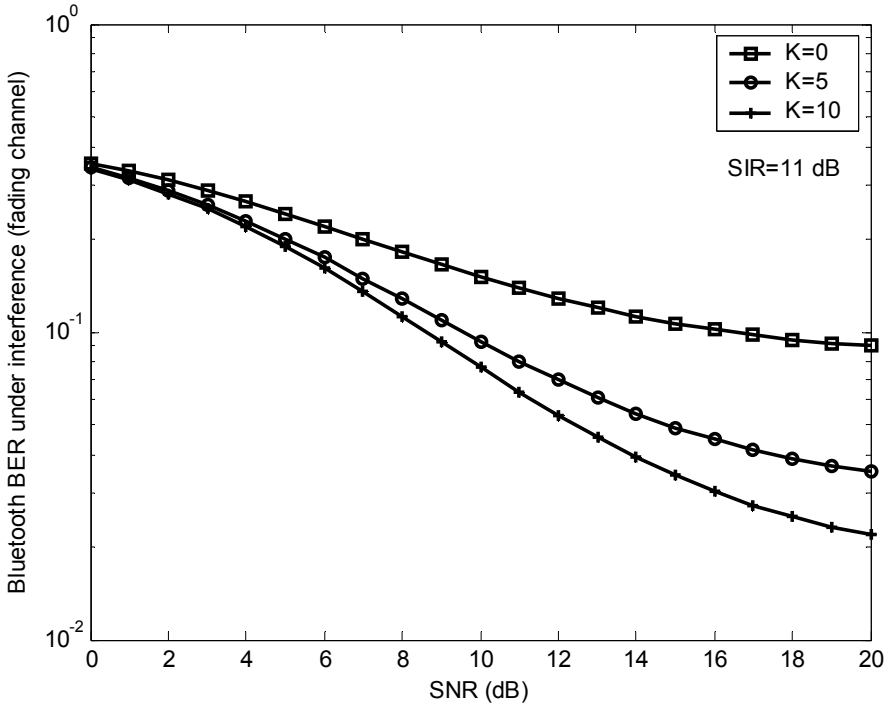

Figure 2.8 Bluetooth BER performance under interference and fading channels

2.5 IEEE 802.11b Overview

Final approval of the IEEE 802.11 standard for WLAN in 1997 has positioned this technology to fulfill the promise of truly mobile computing. The standard discloses WLAN network architecture, including the PHY and the MAC layer specifications. The IEEE 802.11 standard actually provides for three variations of the PHY layer. These include Direct Sequence Spread Spectrum (DSSS), Frequency Hopping Spread Spectrum (FHSS), and Infrared (IR). The basic data rate is 1 Mbps encoded with Differential Binary Phase Shift Keying (DBPSK), and an extended data rate of 2 Mbps using Differential Quadrature Phase Shift Keying (DQPSK). To seek higher data rates allowing wireless functionality comparable to Ethernet, shortly after the IEEE 802.11 standards approved a 1 and 2 Mbps standard for WLANs, a higher rate extension to the physical layer of the standard is named IEEE 802.11b, which applies to wireless LANs and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band [56]. In most of the WLAN products on the market, products based on the IEEE 802.11b technology have a significant presence in practice. Thus in this thesis only 802.11b is considered as our main research object. The first and second rates of 1 and 2 Mbps are achieved by DBPSK and DQPSK with direct sequence spread spectrum using an 11 chip Barker code; the chip rate is 11 Mchips/sec. The third and last rates of 5.5 Mbps, 11 Mbps are obtained using a Complementary Code Keying (CCK) modulator, also achieved at 11 Mchips/sec. A DSSS or CCK transmitter converts the data stream into a symbol stream where each symbol represents a group of bits to spread over a relatively wideband channel. In all modes, the occupied bandwidth is about 22 MHz. With a total bandwidth of 83.5 MHz available in the 2.4 GHz band, there are three non-overlapping channels for IEEE 802.11b system defined in the 2.4 GHz band. The Basic Service Set (BSS) is the fundamental building block

of the IEEE 802.11 architecture. A BSS is defined as a group of stations that are under the direct control of a single coordination function, i.e. a Distributed Coordination Function (DCF) or Point Coordination Function (PCF). The geographical area covered by the BSS is known as the Basic Service Area (BSA), which is analogous to a cell in a cellular communications network. Conceptually, all stations in a BSS can communicate directly with all other stations in a BSS [57].

2.5.1 DSSS

DSSS technique is used to ensure that communications can continue in the presence of an interfering system, although throughput will suffer. DSSS uses a secondary modulation, faster than the information rate, to spread the frequency domain content over a larger band, creating a lower power spectral density. At the DSSS modulator, the information signal is multiplied by a pseudorandom binary-valued sequence that is used to spread the transmitted signal into a symbol stream. The employed pseudorandom sequence has good autocorrelation properties to allow the receiver to recover bit timing. The spreading sequence employed in 802.11b is an 11 chip length Barker sequence, which is c_n = {+1,-1,+1,+1,-1,+1,+1,+1,-1,-1,-1} [56]. The output of the modulator is a spread spectrum signal occupying a wideband channel of 22 MHz. At the receiver, the DSSS demodulator multiplies the received signal by the Barker code sequence. This causes the data signal to be returned to its original form. Signal spreading and despreading schemes can be understood from Figure 2.9. However, DSSS is bandwidth inefficient in that it uses a number of chips to transmit a single bit of information. This inefficiency is the tradeoff to achieve interference rejection, or the ability to have reliable communications even in the presence of an interfering signal. In Figure 2.9, we see the transmitting data signal on the radio channel has a

lower power spectral density covering a larger frequency band. Suppose the spread signal is transmitted in the presence of narrowband interference, the despreading operation at the receiver will recover the wide band spread spectrum signal back to the original data bandwidth, while the narrowband interference is spread to a wide bandwidth, and causes much lower interference to the data signal. The effect of spreading narrowband interference to wide band and despreading information signal back to information band is called processing gain. The processing gain (L_c) of the DSSS system is the ratio of the chip rate to the bit rate, or is usually defined as

$$L_C = \frac{spread \quad bandwidth}{Information \quad bandwidth} \tag{2-25}$$

The 11-chip Barker code using in DSSS of 802.11b increases the processing gain at the receiver of DBPSK system by $10\log\left(\frac{11chips}{1bit}\right) = 10.4dB$. For DQPSK modulation the processing gain is $10\log\left(\frac{11chips}{2bit}\right) = 7.4dB$.

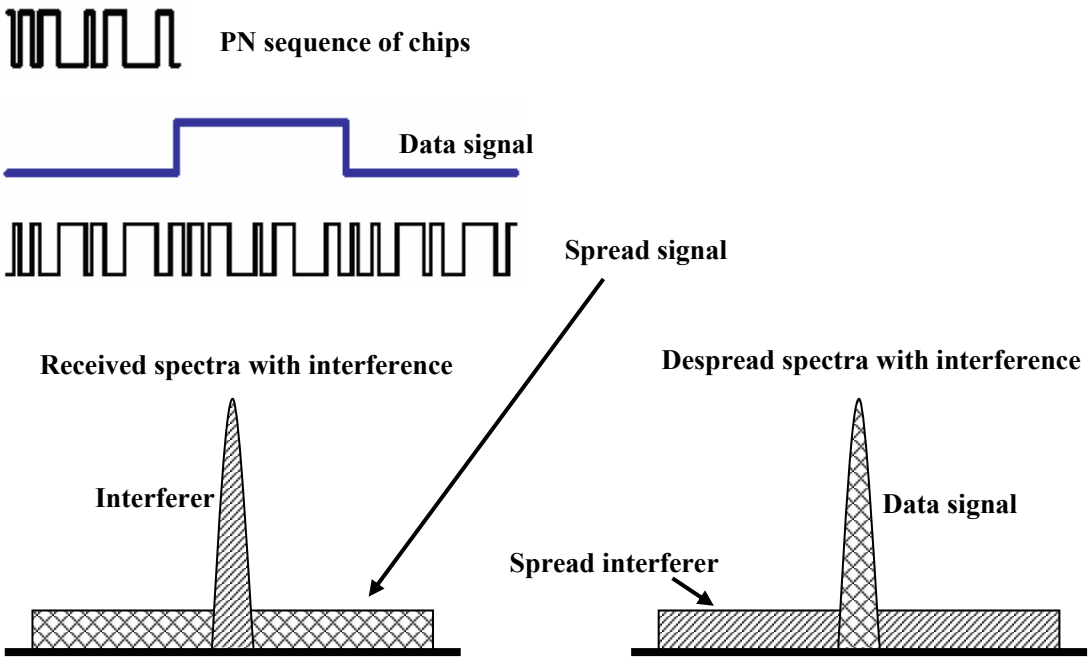

Figure 2.9 Direct sequence spread spectrum

2.5.2 DBPSK and DQPSK Modulations

The operation of Differential Phase Shift Keying (DPSK) modulation can be better explained after understanding the regular Phase Shift Keying (PSK). In a PSK, information of signals is conveyed in a carrier with relative phase shift. For Binary PSK, the pair of signals, 1 or 0, is conveyed in a relative phase shift of 180 degrees; for Quaternary PSK, the signals, 00, 01, 10 or 11, are conveyed in a relative phase shift of 90 degrees. Demodulation is based on the estimation of the carrier phase.

DPSK modulation differs from PSK in a way that there is no direct phase assignment to every symbol; instead, the difference between the current and previous phase is detected and that change in phase indicates the change in the symbol. For example, in the simplest form of DBPSK, 1 may cause a phase shift of π whereas 0 causes no phase change, or vice versa. At the receiver the phase of each symbol is compared with that of the previous symbol, which means that there is a need for delaying the received signal by one symbol length in time. A phase change indicates a 1 is received, no phase change indicates 0. The DPSK is employed in the IEEE 802.11b standard because differential modulation overcomes the need for coherent detection necessary in PSK systems, in other words there is no need for estimation of the carrier phase, and therefore the receiver design is much simpler. Usually the performance of DPSK is 3 dB poorer than that of PSK.

For DBPSK modulation the bit error probability in the AWGN channel is [41]

$$P_e = \frac{1}{2}\exp(-\frac{E_b}{N_0}) \tag{2-26}$$

In the case of DQPSK, the probability of a binary digit error for four-phase DPSK with Gray coding can be expressed as [41]

$$P_e = Q_1(a,b) - \frac{1}{2} I_0(ab) \exp\left(-\frac{1}{2}(a^2 + b^2) \right) \tag{2-27}$$

where $Q_1(a,b)$ and $I_0(ab)$ are as previously defined with parameters a and b defined as

$$a = \sqrt{\frac{2E_b}{N_0} \cdot \left(1 - \sqrt{\frac{1}{2}} \right)} \text{ and } b = \sqrt{\frac{2E_b}{N_0} \cdot \left(1 + \sqrt{\frac{1}{2}} \right)}$$

2.5.3 CCK Modulation

Shortly after the 802.11 standards board approved a 1 and 2 Mbps standard for WLANs in 1997, Harris Semiconductor and Lucent Technologies developed an approach called Complementary Code Keying (CCK) to satisfy increasing market demand for higher data rate WLAN. CCK modulation has the same chip rate and therefore the same bandwidth as the lower rates. This makes it interoperable with the existing 1 and 2 Mbps networks by incorporating the same preamble and header that already has a rate change mechanism. In July 1998, the 802.11 working group adopted CCK as the basis for the high rate PHY layer extension to deliver data rates of 5.5 and 11 Mbps at the 2.4 GHz. CCK abandons spread spectrum techniques in favor of error correction. FCC regulations for the ISM band require at least 10 dB of processing gain. CCK achieves this without being a spread spectrum signal, which is usually defined as processing gain. The processing gain is achieved instead via bandwidth reduction (9dB) and coding gain (2 dB) [58]. Therefore up to 11 times the bit rate could be achieved in the same bandwidth with higher-level modulation and comparable interference rejection.

CCK can be described as a variation of M-ary orthogonal keying using codes with complex symbol structure [58,59]. To easily understand CCK modulation, it is compared to Walsh Codes. Walsh functions were used for M-ary Bi-orthogonal keying (MBOK). They are the most well known orthogonal BPSK vector set and available in 8 chip vectors. A set of *M* Bi-orthogonal signals are constructed from $\frac{1}{2}M$ orthogonal signals by including the negatives of the orthogonal signals. Walsh codes are formed by performing a simple operation as illustrated in Figure 2.10. In a Walsh code structure, the first row has all 1s. Remaining rows contain an equal number of 1s and 0s. For the 8-ary case, there are 8 BPSK chips; each chip has two possible phases, ± 1, that have a maximum vector space of 2^8=256 code words of which one can find sets of 8 that are mutually orthogonal. This 8 mutually orthogonal sets could be picked up from the space as the function of M=8 in Figure 2.10. For CCK, there are 8 complex chips, each chip has four possible phases, ± 1, $\pm j$, that have a maximum vector space of 4^8=65536 possible code words, and sets of 64 that are nearly orthogonal. The 8 complex chips comprise a single symbol. By making the symbol rate 1.375 Msymbol/sec the 11 Mbps waveform ends up occupying the same approximate bandwidth of 22 MHz.

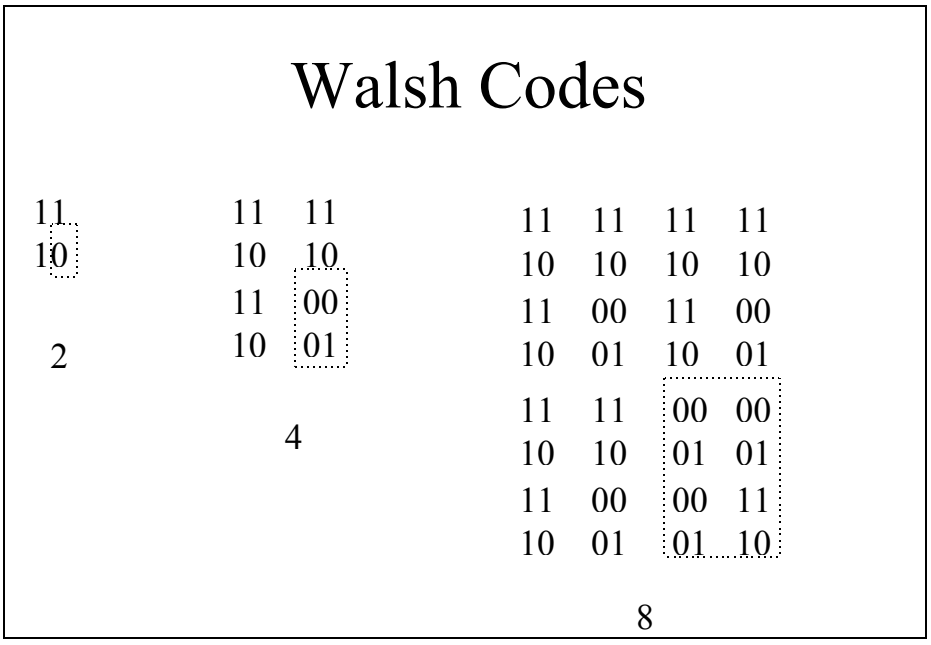

Figure 2.10 Forming Walsh Codes by successive folding

The 8 chips CCK code words are derived from the following formula [60,61]:

$$c = \left\{ e^{j(\varphi_1+\varphi_2+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_3+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_4)}, -e^{j(\varphi_1+\varphi_4)}, e^{j(\varphi_1+\varphi_2+\varphi_3)}, e^{j(\varphi_1+\varphi_3)}, -e^{j(\varphi_1+\varphi_2)}, e^{j\varphi_1} \right\} \quad (2\text{-}28)$$

In it there are 4 phase terms. φ_1 modulates all the chips and is used for the QPSK rotation of the whole code vector. The other three modulate every odd chip (φ_2), every odd pair of chips (φ_3) and every odd quad of chips (φ_4) respectively. The phase of each chip is as follows:

$$\begin{aligned}
\phi_1 &= \varphi_1 + \varphi_2 + \varphi_3 + \varphi_4 \\
\phi_2 &= \varphi_1 + \quad \varphi_3 + \varphi_4 \\
\phi_3 &= \varphi_1 + \varphi_2 \quad + \varphi_4 \\
\phi_4 &= \varphi_1 \quad + \varphi_4 + \pi \\
\phi_5 &= \varphi_1 + \varphi_2 + \varphi_3 \\
\phi_6 &= \varphi_1 \quad + \varphi_3 \\
\phi_7 &= \varphi_1 + \varphi_2 \quad + \pi \\
\phi_8 &= \varphi_1
\end{aligned} \quad (2\text{-}29)$$

The eight equations can be transformed into matrix expression:

$$\begin{pmatrix}\phi_1\\ \phi_2\\ \phi_3\\ \phi_4\\ \phi_5\\ \phi_6\\ \phi_7\\ \phi_8\end{pmatrix}=\begin{bmatrix}1&1&1&1\\ 1&0&1&1\\ 1&1&0&1\\ 1&0&0&1\\ 1&1&1&0\\ 1&0&1&0\\ 1&1&0&0\\ 1&0&0&0\end{bmatrix}\times\begin{pmatrix}\varphi_1\\ \varphi_2\\ \varphi_3\\ \varphi_4\end{pmatrix}+\begin{pmatrix}0\\ 0\\ 0\\ \pi\\ 0\\ 0\\ \pi\\ 0\end{pmatrix} \tag{2-30}$$

The data bit stream is partitioned into 8 bit bytes as $(d7,d6,...,d0)$ where $d0$ is the Least Significant Bit (LSB) and first in time. The 8 bits are used to encode the phase parameters. The phases, φ_1 to φ_4, are defined according to the scheme shown in Table 2.1. Encoding is based on differential QPSK modulation specified in Table 2.2.

Table 2.1 Phase parameter encoding scheme

DIBIT	Phase parameter
$(d1,d0)$	φ_1
$(d3,d2)$	φ_2
$(d5,d4)$	φ_3
$(d7,d6)$	φ_4

Table 2.2 DQPSK modulation of phase parameters

DIBIT(d_{i+1},d_i)	Phase
00	0
01	π
10	$\pi/2$
11	$-\pi/2$

Chip phase generator matrix (Eq. 2-30) can specify 256 code words, but only 64 sets of 256 are nearly orthogonal. To make 11 Mbps CCK modulation, the transmitted data is grouped into 8 bit bytes, where the 6 bits, $d2$ to $d7$, are used to select one of 64 complex vectors of 8 chip length for the symbol and the other 2 bits $(d0,d1)$modulate the entire symbol via QPSK. To get a half data rate version, the 5.5 Mbps CCK mode,

a subset of 4 of the 64 vectors having superior coding distance is used. The incoming data is grouped into 4 bit nibbles, where 2 of those bits select the 8 chips code word out of a set of 4, while the remaining 2 bits modulate the symbol via QPSK. The spreading sequence then modulates the carrier by driving the I and Q modulators via DQPSK [58, 59]. The chip rate is maintained at 11 Mchip/sec for all modes. Figure 2.11 shows the block diagram of the CCK modulator circuit.

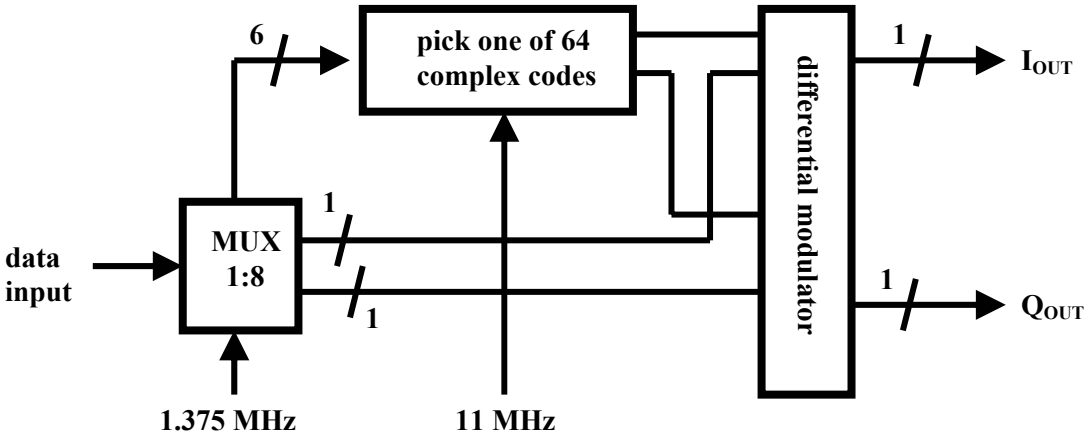

Figure 2.11 Block diagram of HFA3861 modulator circuit

At the demodulator, the optimum receiver correlates the received signal with the codeword set. For the cases where the number of phases M is larger than 2, maximum likelihood decoding becomes too complex for practical implementation. Hence a suboptimum decoding techniques is applied. One way to decode the phases which are applied to all elements of a complementary code is to calculate the phases of complex samples. For the length 8 code with complex samples x_i, the phase equations are given by [60]:

$$\begin{aligned}
\varphi_2 &= \arg\left\{x_1 x_2^* + x_3 x_4^* + x_5 x_6^* + x_7 x_8^*\right\} \\
\varphi_3 &= \arg\left\{x_1 x_3^* + x_2 x_4^* + x_5 x_7^* + x_6 x_8^*\right\} \\
\varphi_4 &= \arg\left\{x_1 x_5^* + x_2 x_6^* + x_3 x_7^* + x_4 x_8^*\right\} \\
\varphi_1 &= \arg\{x_1 e^{-j(\varphi_2+\varphi_3+\varphi_4)} + x_2 e^{-j(\varphi_3+\varphi_4)} + x_3 e^{-j(\varphi_2+\varphi_4)} + x_4 e^{-j(\varphi_4)} \\
&\quad + x_5 e^{-j(\varphi_2+\varphi_3)} + x_6 e^{-j(\varphi_3)} + x_7 e^{-j(\varphi_2)} + x_8\}
\end{aligned} \tag{2-31}$$

where $\arg\{\}$ means calculation of the phase of a complex vector and * denotes the complex conjugate. In order to convert the phases to bits, decisions have to be made concerning which constellation points are closest to the phases found, just as is done in normal phase shift keying. The four phase variables each take on values from $[0, \pi/2, \pi, 3\pi/2]$, and there are 256 (4×64) possible 8 chip codes. Demodulation of the CCK modulated signal is done coherently in the Intersil HFA3861A baseband processor by a RAKE receiver implementation which features a matched filter and Fast Walsh Transform (FWT) block, as be shown in Figure 2.12. A bank of 64 correlators followed by a picker circuit determines which code was transmitted giving 6 bits of the data word (in the 11 Mbps mode). To decode a particular received signal, we correlate the particular code word with the 64 correlators and choose the one that is closest to the received signal, and map that code word back to data bits. The other 2 bits of the 8-bit data word are determined from the QPSK phase of the symbol.

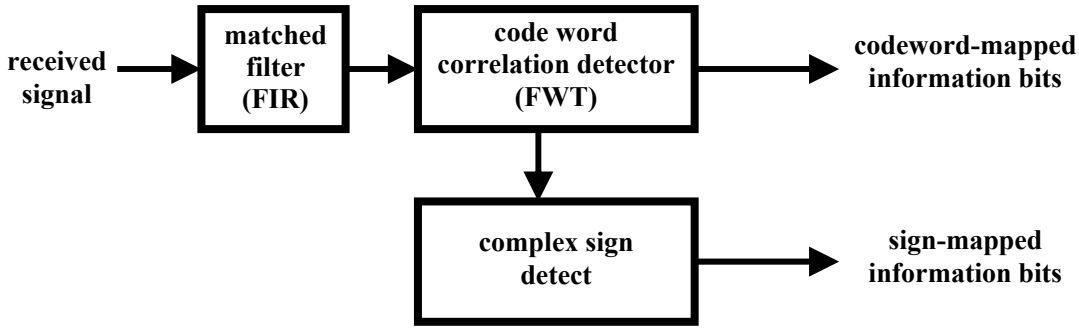

Figure 2.12 HFA3861 RAKE receiver

Instead of getting the processing gain by multiplying a signal with Barker code as 802.11b lower rates, CCK achieves its processing gain by encoding a signal to a spreading code. The spreading code length is 8 chips and based on complementary codes. For the 5.5 Mbps data rate 4 bits are encoded into 8 chip long code word, consequently the code rate is $1/2$. For the 11 Mbps data rate the code rate is 1, since 8 bits are encoded into 8-chip code word. However, when the transmitted information is

coded by the complementary code, the SNR at the output of a soft-decision decoder is increased by the coding gain, defined as [62]

$$G_c = R_c d_{\min} \tag{2-32}$$

where R_c is the code rate and $d_{\min}$ is the minimum Euclidean distance of the code. The minimum distance of CCK can be found by observing that a minimum distance between two code words is obtained if N/2 symbols have a minimum phase rotation of $2\pi / M$, where M is the number of phases. Thus the minimum Euclidean distance $d_{\min}$ is [60]

$$d_{\min} = \sqrt{\frac{N}{2}\left\|1 - \exp(j\frac{2\pi}{M})\right\|} \tag{2-33}$$

For CCK with $N = 8$ and $M = 8$, the minimum distance is 1.53. The subset of 4 vectors for 5.5 Mbps CCK mode is chosen from CCK 64 vectors that having superior coding distance. According to the details in [58], we can assume both CCK modes have the same coding gain. We summarize DSSS and CCK features of 802.11b in Table 2.3.

Table 2.3 DSSS and CCK physical features of 802.11b

data rate (R)	1 Mbps	2 Mbps	5.5 Mbps	11 Mbps
bits/symbol	1 bit	2 bits	4 bits	8 bits
code word chips	11 chips	11 chips	8 chips	8 chips
spreading gain (L_c)	11	5.5	2	1
code gain (G_c)	--	--	1.53	1.53
energy of bit (E_b)	$11E_c$	$5.5E_c$	$2E_c$	E_c
SNR ($G_c \cdot E_b / N_0$)	E_b / N_0	E_b / N_0	$1.53 \cdot E_b / N_0$	$1.53 \cdot E_b / N_0$
SINR $E_b /(N_0 + I_b / L_c)$	$E_b /(N_0 + I_b / 11)$	$E_b /(N_0 + I_b / 5.5)$	$1.53 \cdot E_b /(N_0 + I_b / 2)$	$1.53 \cdot E_b /(N_0 + I_b)$

2.6 Performance of IEEE 802.11b

In this section, the performance of IEEE 802.11b in terms of BER is evaluated under an AWGN channel, Rician and Rayleigh fading channel, as well as the co-channel interference.

2.6.1 Under AWGN Channel

2.6.1.1 DSSS

In an AWGN channel, the probability of error for a DS spread spectrum system employing binary PSK is identical to the probability of error for unspread binary PSK [62]. Therefore, the performance of DBPSK and DQPSK is easily obtained through Eq. (2-26) and Eq. (2-27).

2.6.1.2 CCK

The error probability for CCK modulation is highly dependent on the implementation of the receiver. We establish our analysis based on the RAKE receiver proposed in [61] and [58]. The RAKE receiver is implemented in the PRISM98 chip set which features a matched filter and Fast Walsh Transform block. A bank of 64 correlators followed by a picker circuit determines which code was transmitted giving 6 bits of the data word. The other 2 bits of the 8-bit data word are determined from the QPSK phase of the symbol. So we can suppose the demodulations of DQPSK and CCK are independent, i.e. error probabilities of the first 2 bits and of the remaining bits are independent, we can obtain an average bit error rate for CCK modulation, which is given by:

$$P_e = \frac{2P_1 + kP_2}{2+k} \tag{2-34}$$

where k is the number of data bits (2 or 6) demodulated from CCK code word, P_1 is the average bit error rate for DQPSK (given by Eq. 2-27), P_2 is the average bit error rate for M-ary Orthogonal Keying signals, which is given by [41]

$$P_2 = \frac{2^{k-1}}{2^k - 1} P_M \tag{2-35}$$

where

$$P_M = \frac{1}{2\sqrt{2\pi}} \int_{-\infty}^{\infty} \left[1 - \left(\frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} e^{-\frac{x^2}{2}} dx \right)^{M-1} \right] \exp\left[-\frac{1}{2} \left(y - \sqrt{\frac{2E_s}{N_0}} \right)^2 \right] dy \tag{2-36}$$

Parameters used in equations (2-34) and (2-36) are specified as listed in Table 2.4.

Table 2.4 Parameters for CCK BER calculation

Data rate	k	Code length	E_S	M-ary orthogonal sets
5.5 Mbps	2	8 chips	$2E_b$	4
11 Mbps	6	8 chips	$6E_b$	64

The 802.11b modulations performance in AWGN channel are shown in Figure 2.13. For low SNR, CCK 11 Mbps rate performs best; 5.5 Mbps is second best; then DBPSK and DQPSK. However, as shown in Table 2.3, the average bit energy for higher rates is much weaker than that at lower rates if we assume that the transmit power is fixed. On the other hand, experimental results have showed that higher rates are only desirable for short range operation and fewer interferers. For the latter one, it is because CCK modulation does not have spreading gain at the higher rates, thus its ability to combat interference is worse at higher rates. By considering the average bit energy, CCK actually performs poorer than DSSS, which is shown in Figure 2.14.

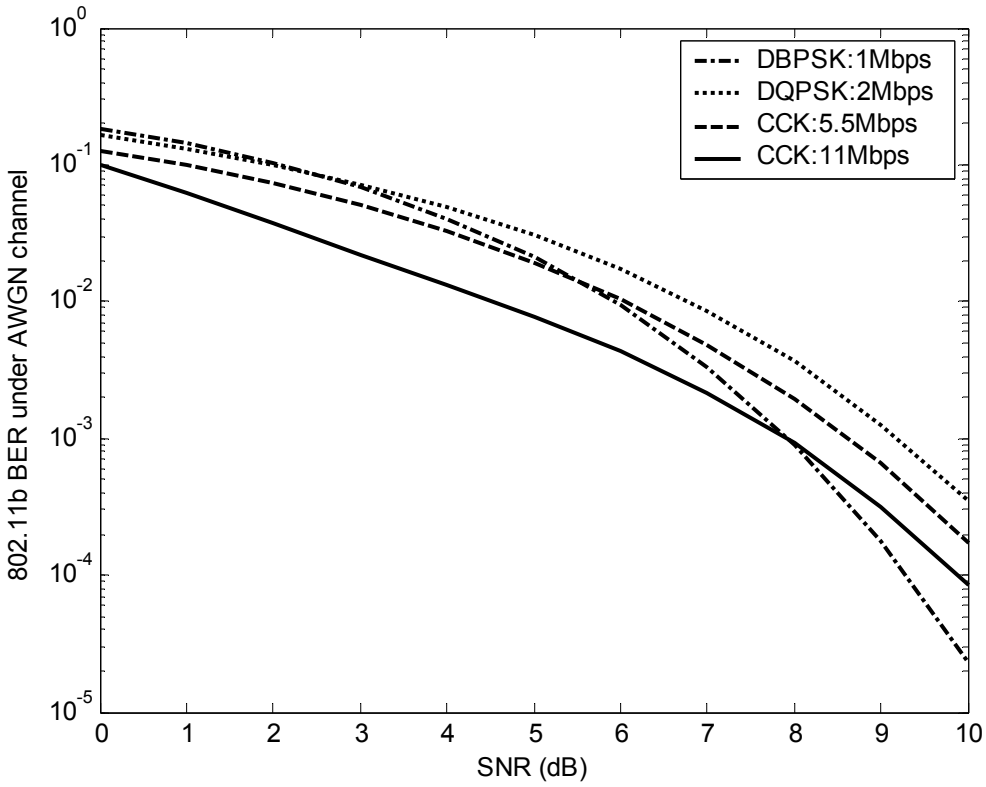

Figure 2.13 802.11b modulations performance under AWGN channel

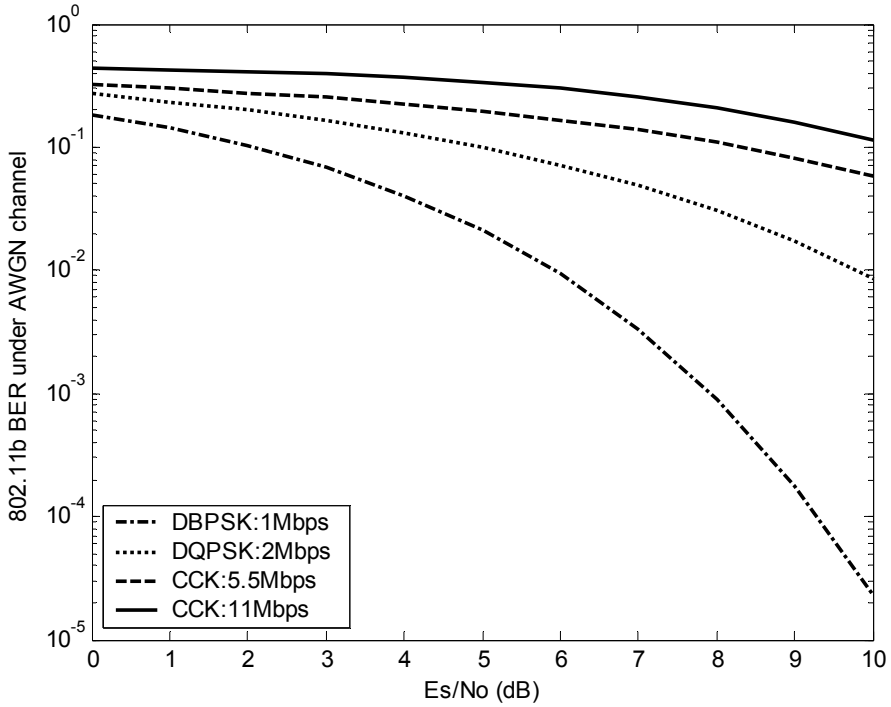

Figure 2.14 802.11b BER performance under AWGN channel of four rates

2.6.2 Under Fading Channel

IEEE 802.11b wireless local area networks are normally deployed in office and housing environments and cover up to 100 meters. The radio channel in indoor environment has been assumed to be flat slow fading and the envelope of the signal associated with the entire packet is multiplied by the same channel gain which is Rayleigh or Rician distributed.

We have given the method to calculate the mean bit error rate of an arbitrary modulation in a fading channel in section 2.1. So we do not repeat it here, and plot the results directly in Figure 2.15. It is found that the performance for 1 Mbps on the Rician (K=10) and Rayleigh fading channel is 3 dB and 6 dB poorer than that on an AWGN channel; the performance for 2 Mbps is 1 dB and 4 dB poorer than that on an AWGN channel; 5.5 Mbps is 1 dB and 2 dB poorer than that on an AWGN channel; and the 11 Mbps does not perform obviously different in fading channel.

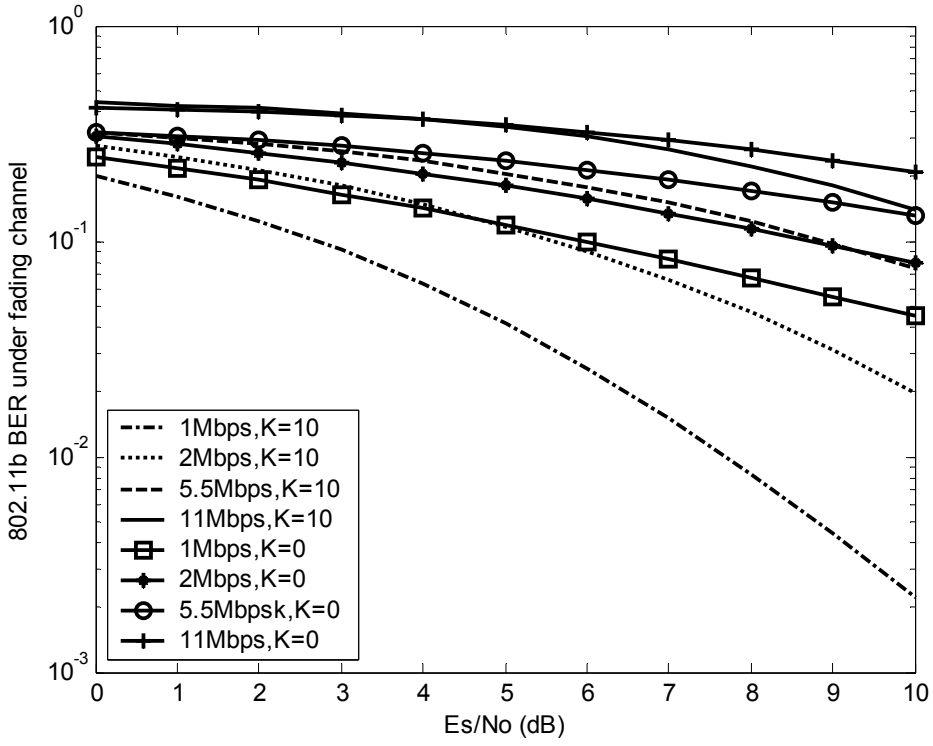

Figure 2.15 802.11b BER performance under fading channel

2.6.3 Under Interference

As the unlicensed 2.4 GHz ISM band opens to a wide variety of signals such as microwave ovens, cordless telephones, WPANs, etc, an 802.11b station will inevitably encounter interference from other devices. We still assume that the interference distribution is Gaussian, therefore the performance of 802.11b in terms of BER can be evaluated under interference. The 802.11b standard does not specify a carrier to co-channel interference ratio for a certain modulation type. Here, we select SIR of 10 dB to evaluate the BER performance under interference. Figure 2.16 shows the BER performance under 10 dB SIR and AWGN channel. Figure 2.17 shows the performance under interference and fading channel.

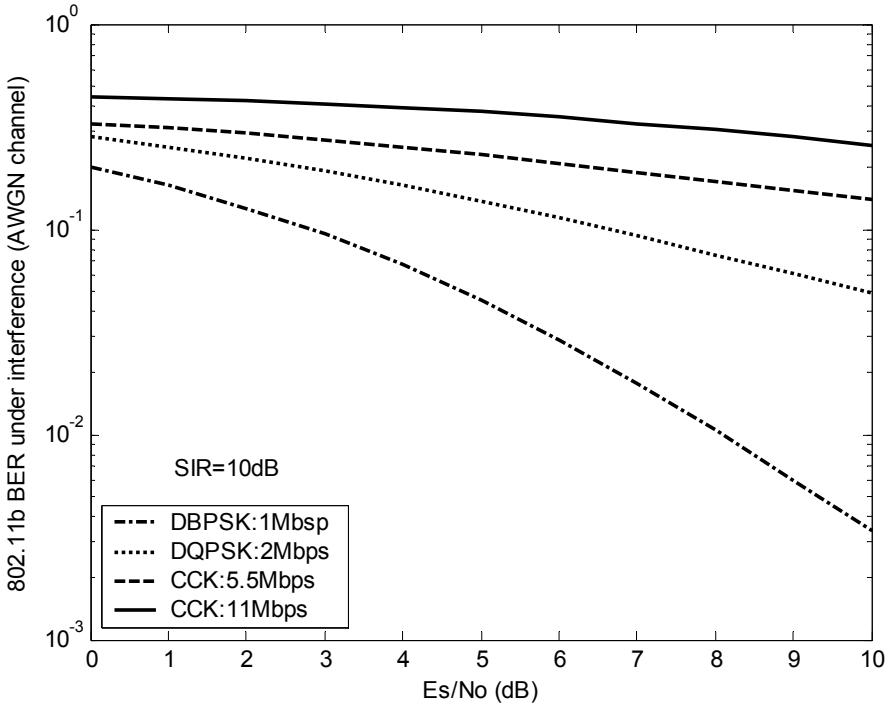

Figure 2.16 802.11b BER performance under interference

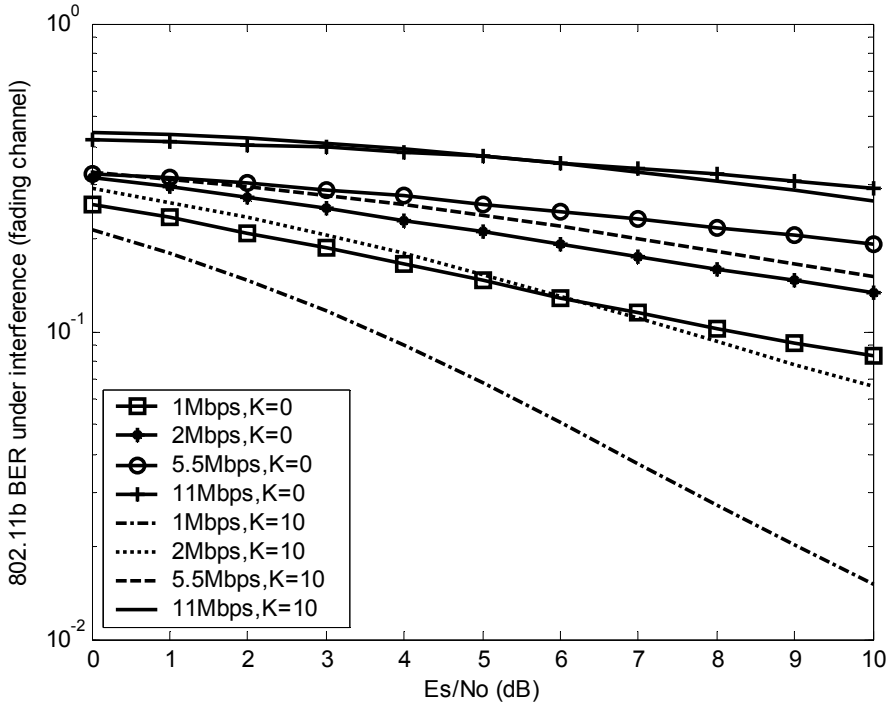

Figure 2.17 802.11b BER performance under interference and fading channels

CHAPTER 3

COLLISION PROBABILITY ANALYSIS IN MAC LAYER

Both systems are operating in the 2.4GHz ISM band. Using FH Spread Spectrum technique, Bluetooth utilizes the whole bandwidth of 2.4GHz ISM band. IEEE 802.11 only occupies 22MHz of the same frequency band. Thus the problem of band sharing occurs. It is worthwhile to note that neither Bluetooth nor 802.11b was designed with specific mechanisms to combat the interference generated by each other, except for some limited interference immunity due to the nature of spread spectrum technology. As a fast frequency hopping system, Bluetooth assumes that it will hop away from bad channels, minimizing its exposure to interference. The 802.11b MAC layer, based on the Ethernet protocol, assumes that many stations share the same medium, and if a transmission fails, it is because two 802.11b stations tried to transmit at the same time.

In order to define mechanisms for the coexistence of IEEE 802.11 and Bluetooth devices operating in a common area, it is imperative to develop an appropriate model to evaluate the effects of their mutual interference, i.e. the interaction of Bluetooth on 802.11b and vice versa. In this chapter we study both systems' collision probability. When studying mutual collision interference, we want to reduce the effects of traffic patterns and concentrate on the effects of time/frequency overlap between the two systems. We make two assumptions: (1) that the 802.11b WLAN is constantly transmitting and (2) that any Bluetooth piconet has packet transmitted in each slot time. These correspond, in some sense, to the worst case scenario. In a real system, there will be times when the interferer is off.

3.1 Bluetooth Channel Definition

Bluetooth technology allows wireless connection set up between Bluetooth-enabled devices. Bluetooth provides for *ad hoc* network structures. The device paging other Bluetooth devices to ask for service could establish a so called piconet, and the paging device is assigned the master role; while the other devices are called slaves. Within a so called piconet, transmission of all units belonging to the same piconet is synchronized. The master unit determines the hopping sequence, the timing, and the scheduling of all packets in the piconet.

There could be a lot of Bluetooth-enabled devices placed in a closed physical area, thus possibly a multi-piconet environment is formed. A FHSS technique allows a Bluetooth transmitter to use the whole 2.4 GHz ISM band by hopping from one frequency to another, but the FH patterns in different piconets are totally incoherent, thus multiple piconets can coexist in a close geographic area and share this 79 MHz frequency band. However, because there is no collaboration among piconets, a desired piconet is possible under interference from other competing piconets. Interference occurs when interfering packets hop to the same frequency of the desired packet at the same time. In this chapter we only consider the collision probability of a piconet in a multi-piconet environment. Whether the collision causes destruction of the packet will be discussed in Chapter 4.

Time-division-duplexing (TDD) is employed in each Bluetooth link. TDD divides the channel in a sequence of slots. Each slot is 625 μs long. By using a polling scheme, the master unit controls all traffic in a piconet. The master transmission is limited to even-numbered slots, while the slave transmission is only permitted to send in odd-numbered slots. Having been selected by the master, the slave is only allowed to

transmit in the immediate successive odd-numbered slot. Thus a Bluetooth device is both a transmitter and a receiver, but not at the same time (half-duplex systems); i.e. in each time there is only one packet transmitting in a piconet, which prevents collision among slaves. The TDD transmission timing is illustrated in Figure 3.1.

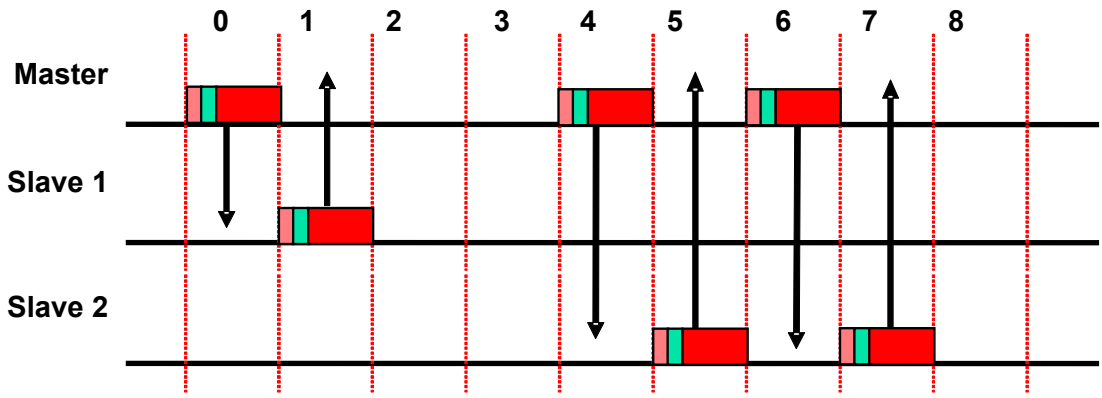

Figure 3.1 Transmission timing example

3.2 802.11 Channel Definition

802.11b physical layer makes use of DSSS at 1 and 2 Mbps data rates, and makes use of CCK scheme at 5.5 and 11 Mbps data rates. A DS transmitter spreads the data stream into wideband symbol spectra with relatively low energy over a relatively wideband channel of 22 MHz; while CCK employs the same chipping rate and spectrum shape as the 802.11 Barker code spread functions. In all modes, the occupied bandwidth is about 22 MHz. Once a link is set up, 802.11b system does not hop. So the collision probability that a 802.11b packet collides with the Bluetooth packet is $22/79$. As the basic medium access control protocol of the 802.11b standard is a Distributed Coordination Function (DCF) that allows for automatic medium sharing through the use of CSMA/CA algorithm, therefore, in each time there is only one

packet allowed to transmit in the channel, which prevents collision among 802.11b stations.

3.3 Collision Probability of Bluetooth

3.3.1 Impact from Competing Piconets

In order to simplify the analysis, we assume that the link is continuously established and every piconet is operating under full traffic load. Full traffic load means there is a packet transmitted in each slot in a piconet. By using TDD scheme, only one packet at most is transmitted in each piconet at a time. We assume a number of piconets coexist with the desired piconet. Two factors affect the collision probability. The first one is that an interfering packet overlaps the desired packet in the same frequency and time. In Bluetooth, a specific frequency hopping pattern is assigned for each piconet. This pattern is determined by the master's identity and clock phase. Change of identity of the piconet will change the hopping sequence, allowing different piconets to operate with different set of random sequences. The frequency hopping strategy used in Bluetooth allows each frequency is visited at an equal probability. Thus the probability that one interfering packet selects the same channel as the desired packet is (1/79). The second factor is that a long packet suffers a larger collision probability than a short packet. A Bluetooth packet can be 1, 3 or 5 time slots long and are transmitted in consecutive slots in the same frequency channel. A desired packet may subject to interfering packets of 1, 3 or 5 time slots long. Thus the collision probability for different packet length is calculated respectively.

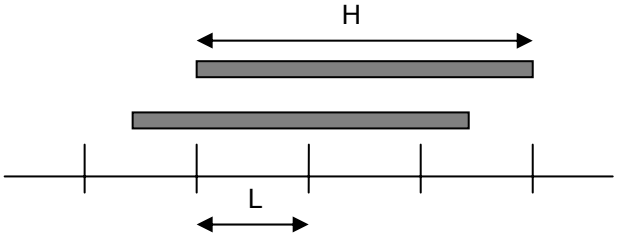

Figure 3.2 Diagram of a Bluetooth packet overlaps a number of hops

Since any two piconets are not synchronized to packet boundaries, and their packet could be any length of 1, 3 or 5 time slots, the desired packet may experience several dangerous hops where the number is dependent not only on the packet length but also on the time offset between the desired and the interfering packets. As shown in Figure 3.2, consider a packet of duration H and let L be the duration of a hop. The minimum number of hops that the packet overlaps is $\lceil H/L \rceil$; in this illustration it is 3. The maximum number of hops that the packet overlaps is $\lceil H/L \rceil + 1$, where $\lceil x \rceil$ is the smallest integer greater than or equal to x. In practice, a transmitted packet includes a data portion and an idle portion. The idle portion is the interval starting from the time that the previous packet finishes to the time that the subsequent packet arrives, which does not include useful information. We denote by T_P the duration of the desired packet transmission and by T_B, the duration of an interfering packet. We denote by T_{BI} the interval between two interfering packets including packet transmission time T_B and an idle period $T_{BI} - T_B$. The actual number of hops that a packet overlaps depends upon the relative timing of the start of the packet and the hop. The values of T_P, T_B and T_{BI} represented in different Bluetooth packet types are given in Table 3.1. Horizontal cells represent the desired packets. Vertical cells represent the interfering

packets. Thus the table shows 1 (3 or 5)-slot packet collided by 1, 3 or 5 slot interfering packet respectively, which totally has nine situations of collision.

Table 3.1 A Bluetooth collided in nine situations

desired / interfering	parameters	1-slot time (μs)	3-slot time (μs)	5-slot time (μs)
1-slot time (μs)	T_P T_B T_{BI}	366 366 625	1622 366 625	2870 366 625
3-slot time (μs)	T_P T_B T_{BI}	366 1622 1875	1622 1622 1875	2870 1622 1875
5-slot time (μs)	T_P T_B T_{BI}	366 2870 3125	1622 2870 3125	2870 2870 3125

- **Collision probability for single time slot packet**

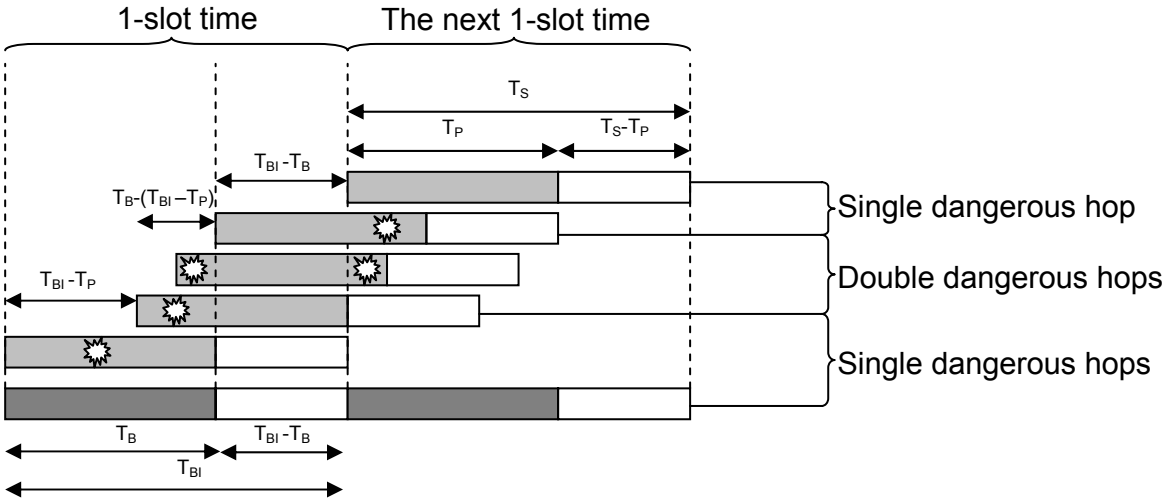

Figure 3.3 Collision exposition for a 1-slot time packet collided by 1-slot time packet

A single time slot packet is the shortest packet length defined in Bluetooth. During the transmission time of the packet, 1-slot packet may overlap a maximum of two ($\lceil T_P / T_{BI} \rceil + 1$) hops. We analyze a 1-slot packet colliding with a 1, 3 or 5 time slots packet through diagram method. Figure 3.3 illustrates a 1-slot packet in collision with

another 1-slot packet. As random arrival time of the two packets, time offset is uniformly distributed between 0 and T_{BI}. In Figure 3.3, all possible overshift of the desired packet is included. We can find that the packet experiences single dangerous hop with a time ratio of $\frac{2T_{BI}-T_P-T_B}{T_{BI}}$; or experiences double dangerous hops with a time ratio of $\frac{T_B-(T_{BI}-T_P)}{T_{BI}}$. Thus the probability that the packet avoids single hop from the hostile piconet is $\frac{2T_{BI}-T_P-T_B}{T_{BI}}\cdot\frac{78}{79}$; the probability that the packet avoids double hops from the hostile piconet is $\frac{T_B-(T_{BI}-T_P)}{T_{BI}}\cdot\left(\frac{78}{79}\right)^2$. Thus the average successful probability of the packet is

$$P_s=\frac{2T_{BI}-T_B-T_P}{T_{BI}}\left(\frac{78}{79}\right)+\frac{T_B-(T_{BI}-T_P)}{T_{BI}}\left(\frac{78}{79}\right)^2 \qquad \text{(3-1a)}$$

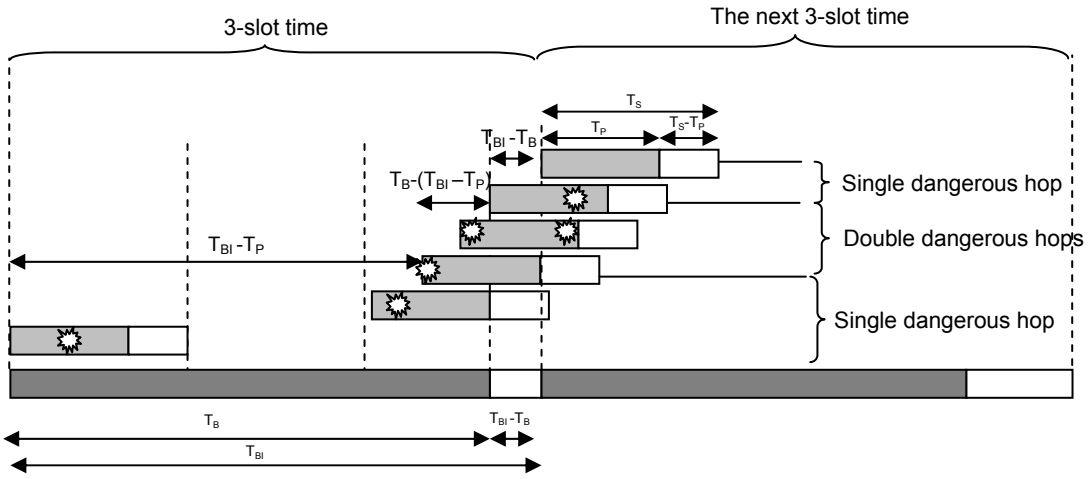

Figure 3.4 Collision exposition for a 1-slot time packet collided by 3-slot time packet

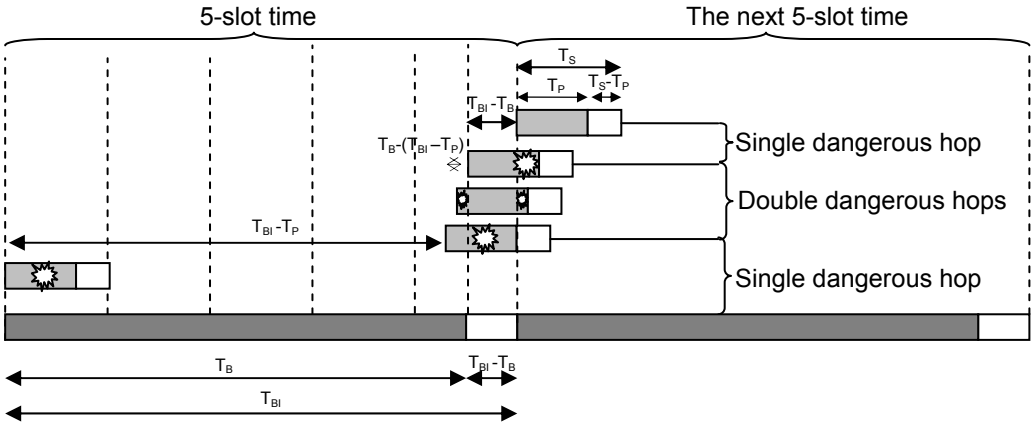

Figure 3.5 Collision exposition for a 1-slot time packet collided by 5-slot time packet

A 1-slot packet collided by 3- or 5-slot packet is illustrated in Figure 3.4 and Figure 3.5 respectively. It is found that the time period of the desired packet collision with single dangerous hop is $2T_{BI} - T_P - T_B$, and collision with double dangerous hops is $T_B - (T_{BI} - T_P)$, which leads to the same successful probability as Eq. 3-1a.

Based on the results, we can straightforwardly extend the conclusion to any packet length which may experience dangerous hops from an interfering packet of the equal or longer length; i.e. in case of $T_P \le T_{BI}$, we obtain the successful probability of the packet is

$$P_s = \frac{2T_{BI} - T_B - T_P}{T_{BI}}\left(\frac{78}{79}\right) + \frac{T_B - (T_{BI} - T_P)}{T_{BI}}\left(\frac{78}{79}\right)^2 \qquad (3\text{-}1b)$$

For coexisting with N piconets, the collision probability of the desired packet is

$$P_c = 1 - \left(P_s\right)^N \qquad (3\text{-}2)$$

The collision probability of a 1-slot packet in the presence of N piconets is shown in Figure 3.6. From Figure 3.6, assuming the collision probability of 0.1 is the least requirement of the performance of system, we can see if it is collided by other 1-slot

packets, the tolerable number of coexisted piconets should not exceed 7; if it is collided by 3 or 5-slot packets, the tolerable number of coexisted piconets should not exceed 8.

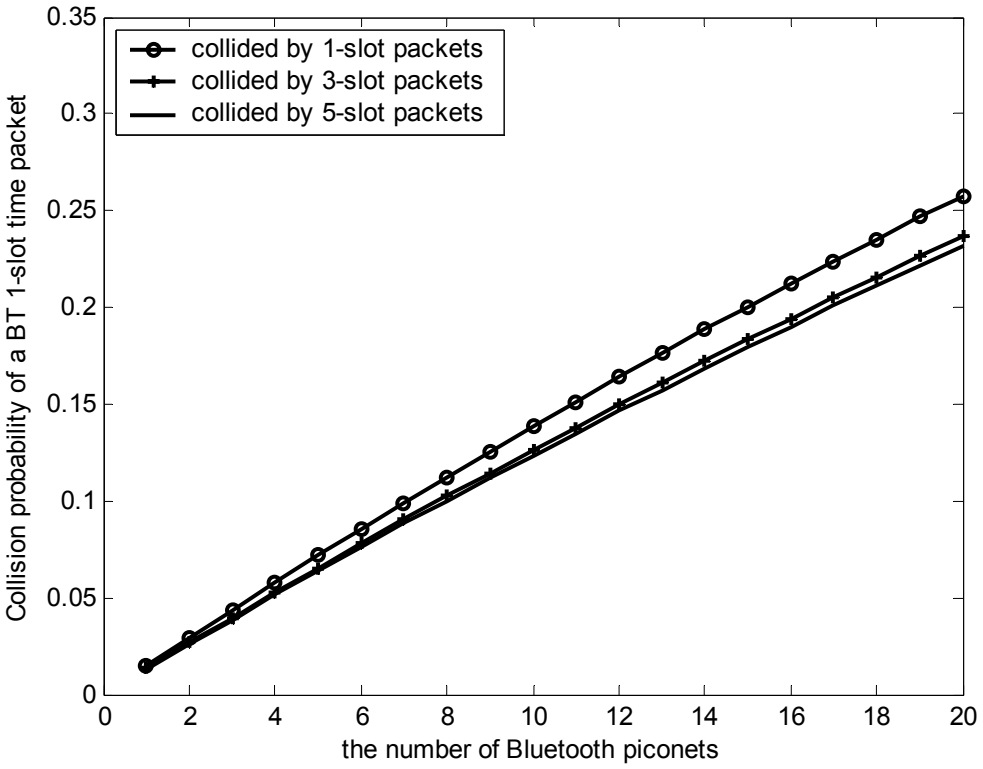

Figure 3.6 Collision probability of a 1-slot time packet

- **Collision probability for 3 time slots packet**

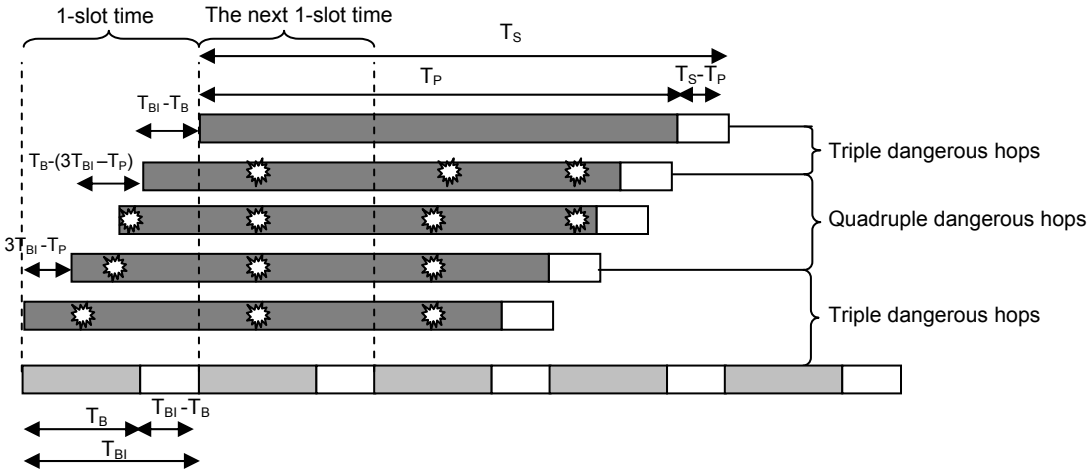

Figure 3.7 Collision exposition for a 3-slot time packet collided by 1-slot time packet

A 3 time slots packet occupies 3 successive slots long in the same frequency channel. During the transmission time of the packet, the number of hops from a 3- or 5-slot packet is a maximum of two ($\lceil T_P / T_{BI} \rceil + 1$); the number of hops from 1-slot packet is a maximum of four and a minimum of three. As we have discussed above, for $T_P \le T_{BI}$, P_s is $\frac{2T_{BI} - T_B - T_P}{T_{BI}}\left(\frac{78}{79}\right) + \frac{T_B - (T_{BI} - T_P)}{T_{BI}}\left(\frac{78}{79}\right)^2$. Therefore, let us see what is the collision probability of a 3-slot packet collided by a 1-slot packet. Still we use diagram to illustrate this collision situation. In Figure 3.7, all possible shifts of the desired packet over a 1-slot interfering packet are included. We can find that the packet experiences triple dangerous hops with a time ratio of $\frac{4T_{BI} - T_P - T_B}{T_{BI}}$; or experiences quadruple dangerous hops with a time ratio of $\frac{T_B - (3T_{BI} - T_P)}{T_{BI}}$. The probability that the packet avoids triple hops from the hostile piconet

is $\frac{4T_{BI}-T_P-T_B}{T_{BI}}\cdot\left(\frac{78}{79}\right)^3$; the probability of avoiding quadruple hops from the hostile piconet is $\frac{T_B-(3T_{BI}-T_P)}{T_{BI}}\cdot\left(\frac{78}{79}\right)^4$. Thus successful probability of the packet is

$$P_s=\frac{4T_{BI}-T_B-T_P}{T_{BI}}\left(\frac{78}{79}\right)^3+\frac{T_B-(3T_{BI}-T_P)}{T_{BI}}\left(\frac{78}{79}\right)^4 \tag{3-3}$$

For coexisting with N piconets, the collision probability is Eq. (3-2).

The collision probability of a 3 time slots packet as the function of piconets is shown in Figure 3.8. From Figure 3.8, assuming the collision probability of 0.1 is the least requirement of the performance of system, we can see if it is collided by other 1-slot packets, the tolerable number of coexisted piconets should not exceed 3; if it is collided by 3 and 5-slot packets, the tolerable number of coexisted piconets should not exceed 5 and 6.

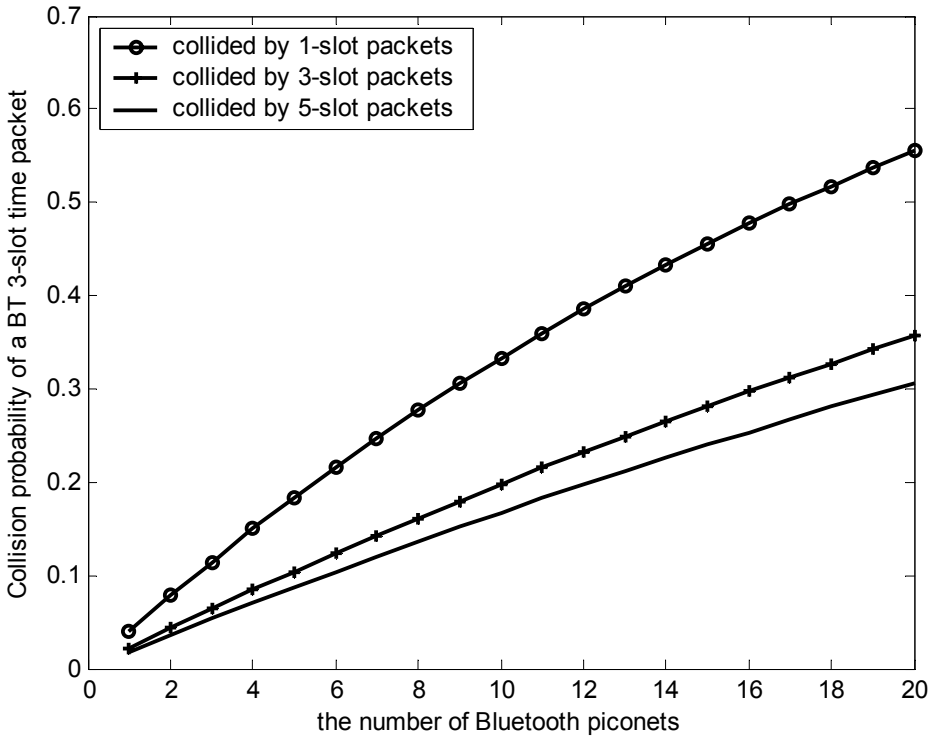

Figure 3.8 Collision probability of a 3-slot time packet

- **Collision probability for 5 time slots packet**

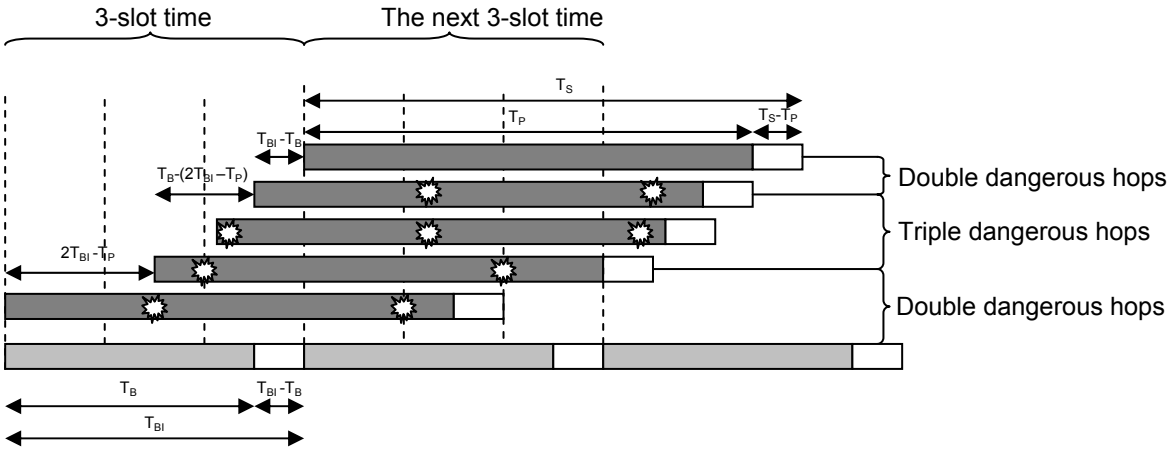

Figure 3.9 Collision exposition for a 5-slot time packet collided by 3-slot time packet

A 5 time slots packet occupies 5 successive slots long in the same frequency channel. During the transmission time of the packet, the number of hops from 5-slot packet is a maximum of two; the number of hops from 3-slot packet is a maximum of 3 and a minimum of 2; the number of hops from 1-slot packet is a maximum of 6 and a minimum of 5. For the packet collided by a 5-slot packet, equal length of two packets results in $P_s = \frac{2T_{BI} - T_B - T_P}{T_{BI}}\left(\frac{78}{79}\right) + \frac{T_B - (T_{BI} - T_P)}{T_{BI}}\left(\frac{78}{79}\right)^2$. Now let us see what is the collision probability that the packet collided by a 3-slot packet. We use diagram to illustrate this collision situation. In Figure 3.9, all possible shifts of the desired packet over the interfering packet are included. We can find that the packet experiences double dangerous hops with a time ratio of $\frac{3T_{BI} - T_P - T_B}{T_{BI}}$; or experiences triple dangerous hops with a time ratio of $\frac{T_B - (2T_{BI} - T_P)}{T_{BI}}$. The probability that the packet avoids triple hops from the hostile piconet is $\frac{3T_{BI} - T_P - T_B}{T_{BI}} \cdot \left(\frac{78}{79}\right)^2$; the probability of

avoiding quadruple hops from the hostile piconet is $\frac{T_B-(2T_{BI}-T_P)}{T_{BI}}\cdot\left(\frac{78}{79}\right)^3$. Thus successful probability of the packet is

$$P_s=\frac{3T_{BI}-T_B-T_P}{T_{BI}}\left(\frac{78}{79}\right)^2+\frac{T_B-(2T_{BI}-T_P)}{T_{BI}}\left(\frac{78}{79}\right)^3 \tag{3-4}$$

Preventing reduplicate work, we do not draw the diagram for the packet collided by a 1-slot packet. Instead, we give P_s directly as follows:

$$P_s=\frac{6T_{BI}-T_B-T_P}{T_{BI}}\left(\frac{78}{79}\right)^5+\frac{T_B-(5T_{BI}-T_P)}{T_{BI}}\left(\frac{78}{79}\right)^6 \tag{3-5}$$

For coexisting with N piconets, the collision probability of the desired packet is Eq. (3-2). The collision probability of a 5 time slots packet as the function of piconets is shown in Figure 3.10. From Figure 3.10, assuming the collision probability of 0.1 is the least requirement of the performance of system, we can see if it is collided by 1-slot packets, the tolerable number of coexisted piconets should not exceed 2; if it is collided by 3-slot packets, the tolerable number of coexisted piconets should not exceed 3; and if it is collided by 5-slot packets, the tolerable number of coexisted piconets should not exceed 4. The coexistence number of piconets is summarized in Table 3.2.

Table 3.2 The tolerable coexistence number of piconets for different packet types

1-slot packet	3-slot packet	5-slot packet	conditions
Co-work with 7 piconets	Co-work with 3 piconets	Co-work with 2 piconets	collided by 1-slot packets
Co-work with 8 piconets	Co-work with 5 piconets	Co-work with 3 piconets	collided by 3-slot packets
Co-work with 8 piconets	Co-work with 6 piconets	Co-work with 4 piconets	collided by 5-slot packets

Up to now we find that a longer Bluetooth packet suffers danger of more collision. However, on the other side, to reduce the interference from competing piconets, longer packets are suggested to use for those interfering piconets. To balance this conflict and maintain fairness among all the piconets, we find 1-slot packet type is the optimal to each piconet for high density piconets coexistence scenario; 3-slot packet type is optimal for moderate density piconets coexistence scenario; while 5-slot packet type is optimal only in the scenario where there are few competitors.

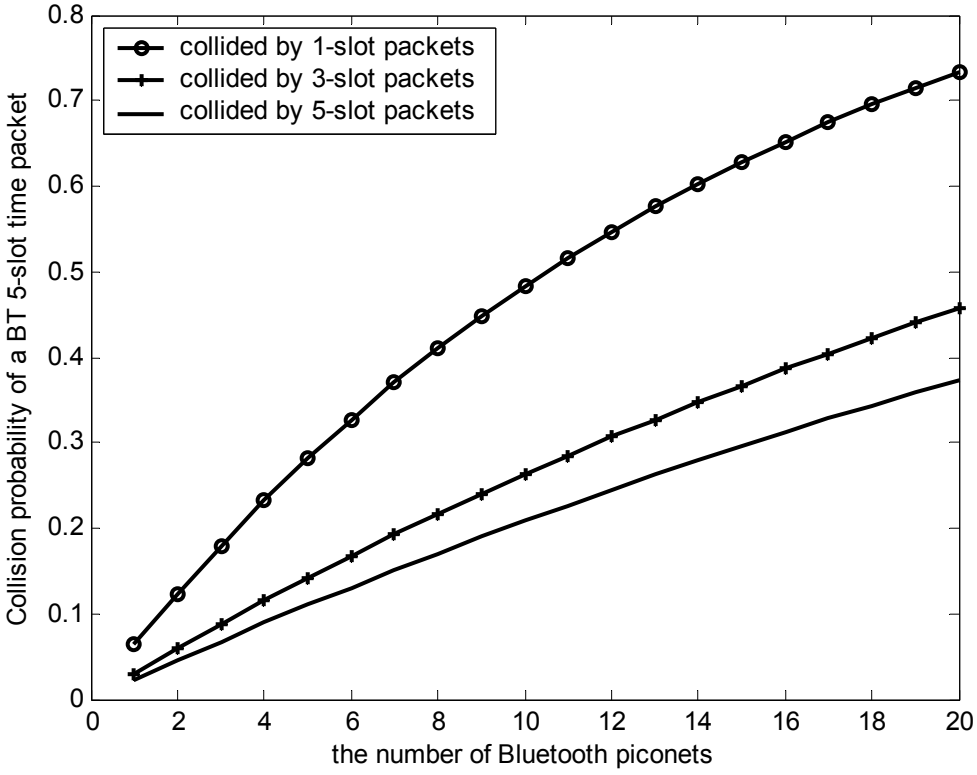

Figure 3.10 Collision probability of a 5-slot time packet

- **A General Expression of the Collision Probability**

Observing equations (3-1) and (3-3) to (3-5), it is found that all four equations have the same form. If we substitute the number of dangerous hops with $\lceil T_P / T_{BI} \rceil$

or $\lceil T_P / T_{BI} \rceil + 1$, we can obtain a general formula for collision probability, where P_s is given

$$P_s = \frac{\left(\lceil T_P / T_{BI} \rceil + 1\right) \cdot T_{BI} - T_B - T_P}{T_{BI}} \left(\frac{78}{79}\right)^{\lceil T_P / T_{BI} \rceil} + \frac{T_B - (\lceil T_P / T_{BI} \rceil \cdot T_{BI} - T_P)}{T_{BI}} \left(\frac{78}{79}\right)^{\lceil T_P / T_{BI} \rceil + 1} \tag{3-6}$$

Given any Bluetooth packet length, Eq. (3-6) can be used to calculate the collision probability of a Bluetooth packet in various scenarios.

3.3.2 Impact from 802.11b

The interference from 802.11b with Bluetooth is termed frequency static interference because they are always from a fixed frequency band. We assume that the 802.11b network has full traffic load, i.e. a packet is transmitted immediately following the previous one. The packet format supported by IEEE 802.11b comprises a preamble, header and frame body. The preamble and header of the frame are always transmitted using DBPSK at 1Mbps, while data packets can be configured for DBPSK, DQPSK or CCK. Consequently an 802.11b packet transmission time is dependent on the data frame length and data rate used. In the analysis, 802.11b packets are assumed to use fixed packet length when a link is setup between two stations and 802.11b packets do not hop. The collision between Bluetooth and 802.11b happens when a Bluetooth packet hops to the same frequency channel of an 802.11b packet. The probability is 22/79. The Bluetooth packet can be 1, 3 or 5 slots long and subjects to interfering packets of different lengths from 802.11b. Figure 3.11 illustrates the timing of the Bluetooth packet with respect to 802.11b packets. We denote by T_B and T_W, the Bluetooth and the 802.11b packet transmission periods, respectively. We denote

by T_{WI}, the interval between two 802.11b packets including the packet transmission time T_W and a backoff period $T_{backoff}$. $T_{backoff}$ considered here is the sum of several variables such as SIFS, DIFS, the ACK transmission time, and CW. These parameters of 802.11b are defined in Subsection 3.4.1, and their values are listed in Table 3.3 [18][31][57]. Similarly, T_{BI} denotes the interval of a Bluetooth packet transmission with idle time.

Table 3.3 802.11b simulation parameters

a Slot Time	SIFS Time	DIFS Time	CW_{min} (slot times)	CW_{max} (slot times)	ACK
$20\mu s$	$10\mu s$	$50\mu s$	31	1023	$112\mu s$

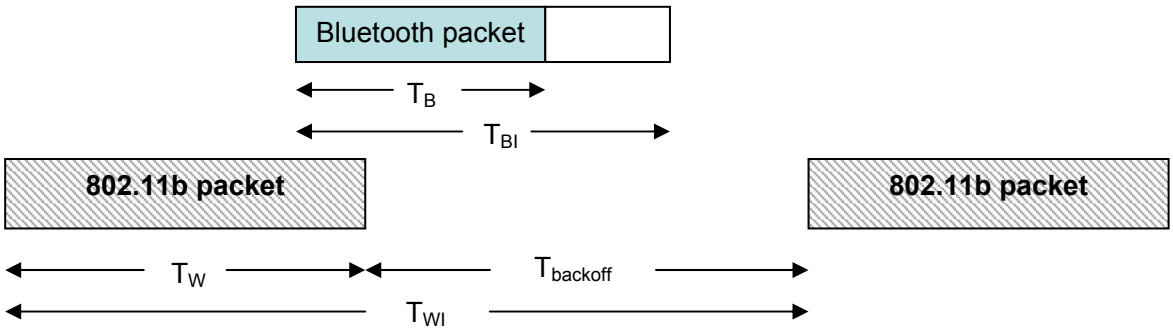

Figure 3.11 Collision of 802.11b packet on Bluetooth

Because of the presence of $T_{backoff}$, when the Bluetooth packet hops during the duration of $T_{backoff}$, there is no effect on the Bluetooth packet. The analysis is similar to that in Subsection 3.3.1. As 802.11b packets do not hop, a Bluetooth packet only experiences one hop danger, which is that the Bluetooth packet hops in the 802.11b network channel. Regardless of the 802.11 packet length, there are only two cases to be considered, i.e. $T_B > T_{backoff}$ and $T_B \le T_{backoff}$. Thus collision probability of a Bluetooth packet interfered by an 802.11b packet is given as

$$P_c = \begin{cases} \dfrac{22}{79} & T_B > T_{backoff} \\ 1 - \left[\left(\dfrac{T_B + T_W}{T_{WI}} \right) \cdot \left(\dfrac{57}{79} \right) + \dfrac{T_{backoff} - T_B}{T_{WI}} \cdot \left(\dfrac{57}{79} \right)^0 \right] & T_B \le T_{backoff} \end{cases} \quad (3\text{-}7)$$

The collision probability of a Bluetooth packet as the function of 802.11 packet length is shown in Figure 3.12. $T_{backoff}$ used here is selected an average value which is given by $\overline{T}_{backoff} = SIFS + DIFS + 32 \cdot aSlotTime + ACK$. From the result, we can see that the collision probability of 1-slot packet correlates with the length of an 802.11b packet. But for 3 or 5-slot time packet, it is a constant because their length is longer than $T_{backoff}$. We can see the effect from 802.11b is limited to Bluetooth. It cannot be worse than $\frac{22}{79}$.

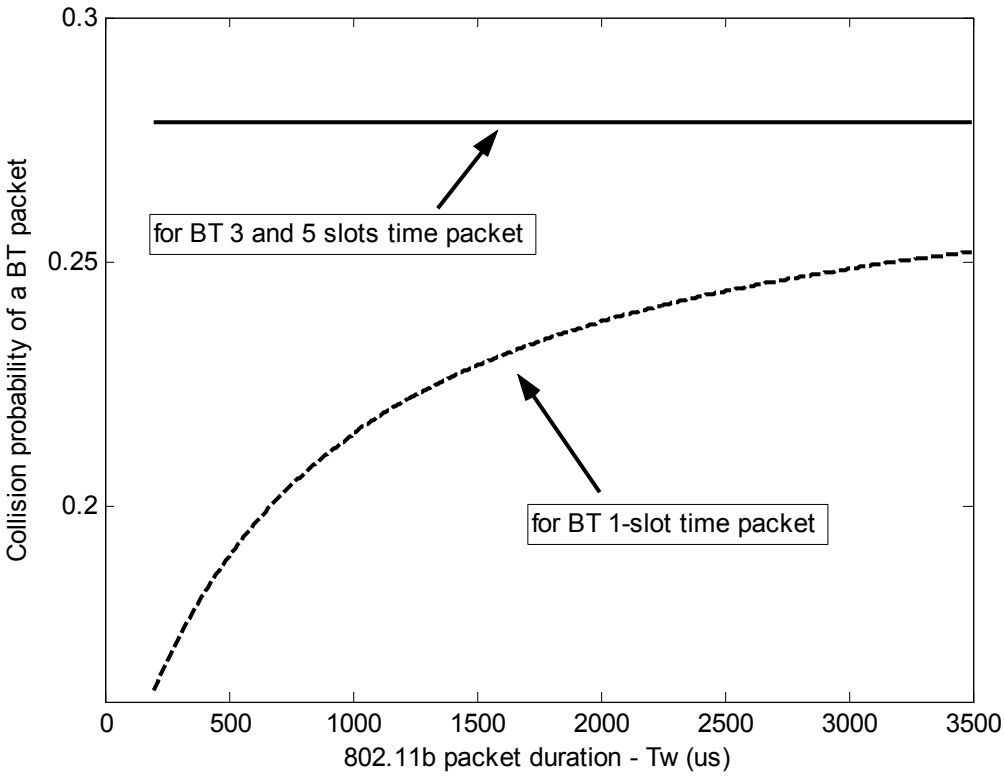

Figure 3.12 Collision probability of a Bluetooth packet in the presence of 802.11b

3.4 Collision Probability of 802.11b

3.4.1 Impact from Other 802.11b Stations

The IEEE 802.11 MAC layer specifications common to all PHY layers and data rates coordinate the communication between stations and control the behavior of users who want to access the network. Two fundamentally different MAC schemes, the Distributed Coordination Function (DCF) and the Point Coordination Function (PCF), are supported to transport asynchronous and time bounded services. The DCF is the fundamental access method used to support asynchronous data transfer on a best effort basis. The PCF is an optional capability, which is connection-oriented, and provides contention-free (CF) frame transfer. The DCF which describes the default MAC protocol operation is based on a scheme known as Carrier-Sense Multiple Access, with Collision Avoidance (CSMA/CA). Both the MAC and PHY layers cooperate in order to implement collision avoidance procedures. The PHY layer samples the received energy over the medium transmitting data and uses a Clear Channel Assessment (CCA) algorithm to determine if the channel is clear. This is accomplished by measuring the RF energy at the antenna and determining the strength of the received signal commonly known as Received Signal Strength Indicator (RSSI). In addition, carrier sense can be used to determine if the channel is available. This technique is more selective since it verifies that the signal is the same carrier type as 802.11 transmitters [18]. Figure 3.13 is a timing diagram illustrating the successful transmission of a data frame. When the data frame is transmitted, the duration field of the frame is used to let all stations in the BSS know how long the medium will be busy. All stations hearing the data frame adjust their Network Allocation Vector (NAV) based on the duration field value, which includes the SIFS interval and the ACK following the data frame [57].

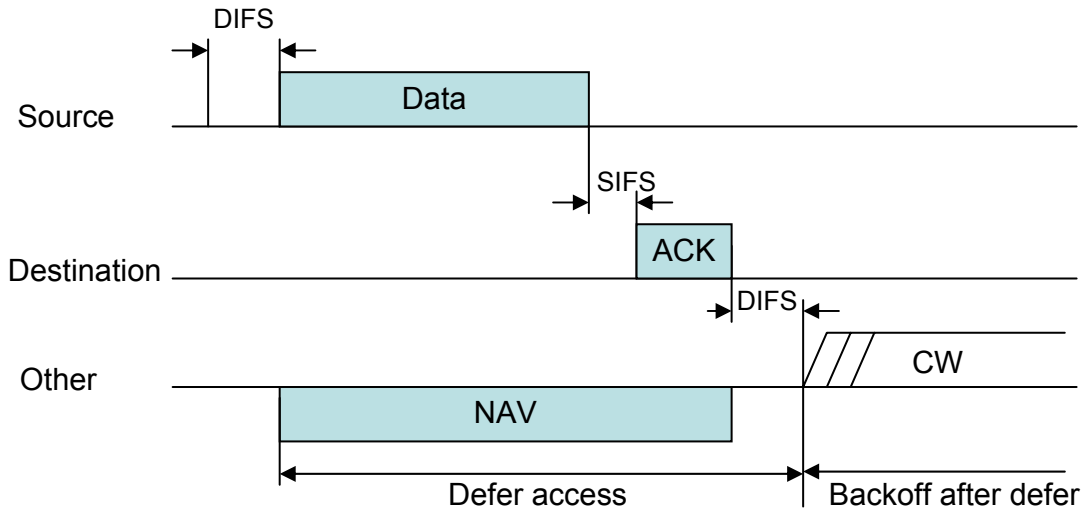

Figure 3.13 Transmission of an 802.11 frame without RTS/CTS

Since a source station in a BSS cannot hear its own transmissions, when a collision occurs, the source continues transmitting the complete frame. Then a virtual carrier sense mechanism is also provided at the MAC layer. It uses the request-to-send (RTS) and clear-to-send (CTS) message exchange to make predictions of future traffic on the medium and updates the NAV available in other stations. The RTS control frame is first transmitted by the source station. All stations in the BSS, hearing the RTS packet, set their NAVs accordingly. The destination station responds to the RTS packet with a CTS packet. Upon successful reception of the CTS, the source station is virtually assured that the medium is stable and reserved for successful transmission of the frame. Figure 3.14 illustrates the transmission of a frame using the RTS/CTS mechanism. If the CTS frame is not received, it is assumed that a collision occurred and the RTS process starts over [57].

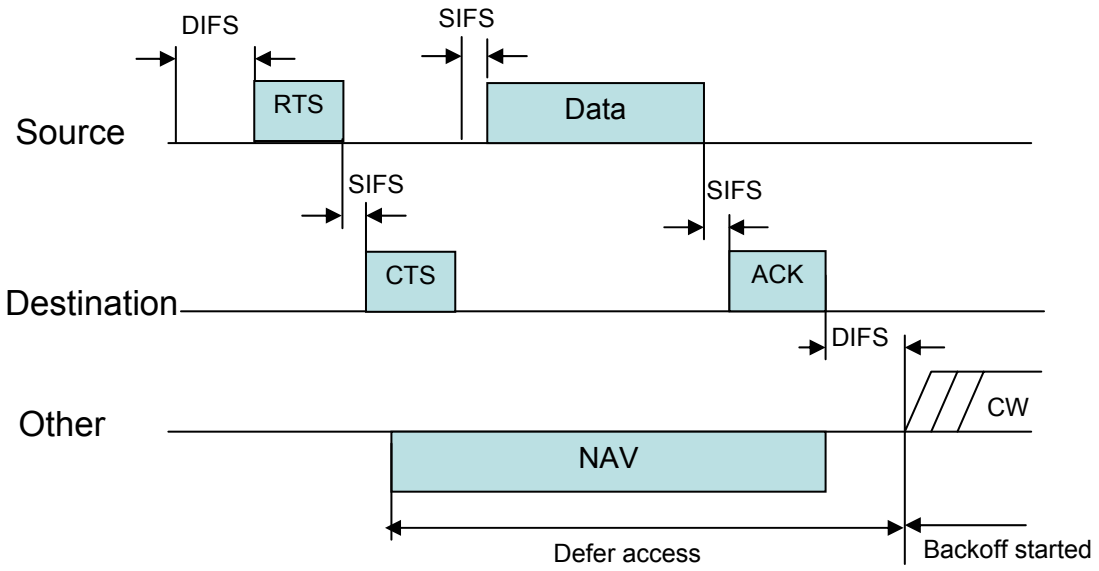

Figure 3.14 Transmission of an 802.11 frame using RTS/CTS

Regardless of whether the virtual carrier sense routine is used or not, the MAC is required to implement a basic access procedure (depicted in Figure 3.15) as follows. If a station has data to send, it waits for the channel to be idle through the use of the CSMA/CA algorithm. If the medium is sensed idle for a period greater than a DCF interframe space (DIFS), the station goes into a backoff procedure before it sends its frame. Upon the successful reception of a frame, the destination station returns an ACK frame after a short interframe space (SIFS). The backoff window is based on a random value uniformly distributed in the interval [0, CW] where CW represents the contention window parameter and is varied between $CW_{\min}$ and $CW_{\max}$. If the medium is determined busy at any time during the backoff slot, the backoff procedure is suspended. It is resumed after the medium has been idle for the duration of the DIFS period. If an ACK is not received within an ACK timeout interval, the station assumes that either the data frame or the ACK was lost and needs to retransmit its data frame by repeating the basic access procedure [18]. Therefore, collision between 802.11b stations is not considered in this thesis.

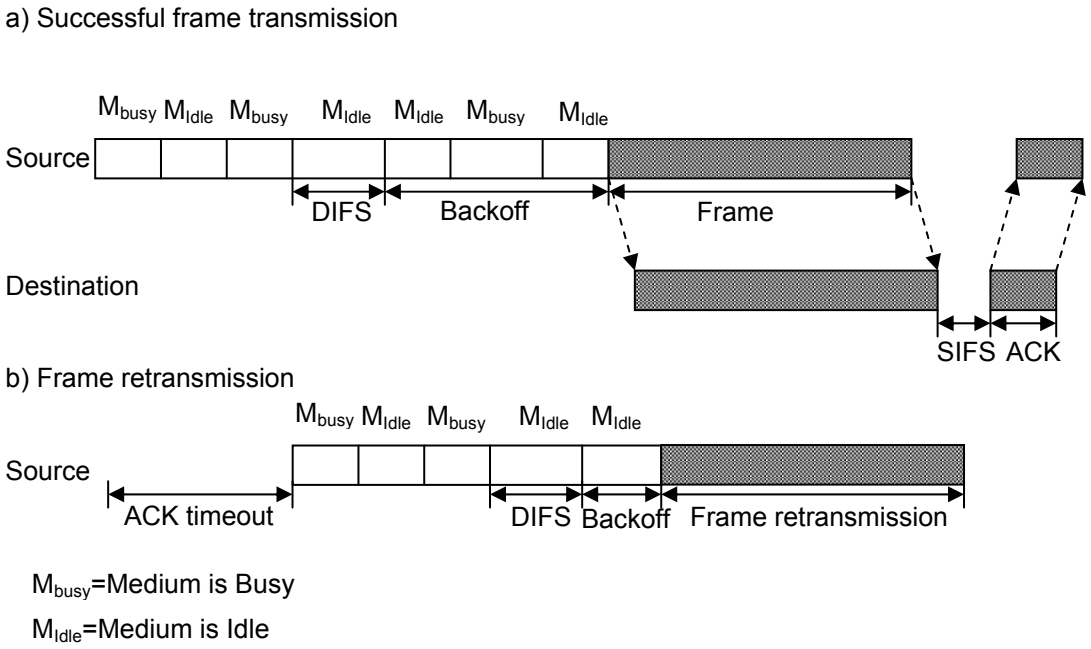

Figure 3.15 WLAN frame transmission scheme

3.4.2 Impact from Bluetooth Piconets

We assume that the CSMA/CA scheme in 802.11b is capable of detecting other 802.11 devices of the same kind but cannot detect the presence of Bluetooth devices. The analysis of reverse effect that Bluetooth piconets impact on an 802.11 network is studied in this subsection.

We assume a number of piconets coexist with the desired 802.11b network. In order to simplify the analysis, we assume that the link is continuously established and every piconet is in full traffic load. By using TDD scheme, only one packet is transmitting in each piconet at a time. Transmission duration of the desired 802.11b packet can be of any length and subject to interfering packet of 1, 3 or 5 time slots long. As we know, Bluetooth packets hop from one channel to another. During the 802.11b packet transmission time, the packet may experience a number of hops from Bluetooth packets. The problem could be even more complex because the length of an 802.11b

packet is not constant and is dependent on the data frame length and data rate used. Three cases are thus considered: (i) $T_W \le T_{BI}$; (ii) $T_{BI} < T_W \le 2T_{BI}$; and (iii) T_W and T_{BI} of any length. T_W denotes the 802.11b packet duration; T_B denotes a Bluetooth packet duration, and T_{BI} denotes the interval between two consecutive Bluetooth packets.

Case (i)

- When $T_W > T_{BI} - T_B$, we find that the packet experiences single dangerous hop with a time ratio of $\frac{2T_{BI} - T_B - T_W}{T_{BI}}$; or experiences double dangerous hops with a time ratio of $\frac{T_B - (T_{BI} - T_W)}{T_{BI}}$. The probability that the packet avoids single hop from the hostile piconet is $\frac{2T_{BI} - T_B - T_W}{T_{BI}} \cdot \frac{57}{79}$; the probability of avoiding double hops from the hostile piconet is $\frac{T_B - (T_{BI} - T_W)}{T_{BI}} \cdot \left(\frac{57}{79}\right)^2$. Hence the successful probability of the packet not to be disturbed by a Bluetooth piconet is given by

$$P_s = \frac{2T_{BI} - T_B - T_W}{T_{BI}} \times (57/79) + \frac{T_B - (T_{BI} - T_W)}{T_{BI}} \times (57/79)^2 \qquad (3\text{-}8)$$

- When $T_W \le T_{BI} - T_B$, there is a time ratio of $\frac{T_W + T_B}{T_{BI}}$ that the packet experiences single dangerous hop and a time ratio of $\frac{T_{BI} - T_W - T_B}{T_{BI}}$ that the packet does not experience any hop. Hence the successful probability of the packet not to be disturbed by a Bluetooth piconet is given by

$$P_s = \frac{T_W + T_B}{T_{BI}} \times (57/79) + \frac{T_{BI} - T_W - T_B}{T_{BI}} \times (57/79)^0 \qquad (3\text{-}9)$$

Case (ii)

- When $2T_{BI} - T_B < T_W$, there is a time ratio of $\frac{3T_{BI} - T_W - T_B}{T_{BI}}$ that the packet experiences double dangerous hops and a time ratio of $\frac{T_B - (2T_{BI} - T_W)}{T_{BI}}$ that the packet experiences triple dangerous hops. Hence the successful probability of the packet not to be disturbed by a Bluetooth piconet is given by

$$P_s = \frac{3T_{BI} - T_W - T_B}{T_{BI}} \times (57/79)^2 + \frac{T_B - (2T_{BI} - T_W)}{T_{BI}} \times (57/79)^3 \qquad (3\text{-}10)$$

- When $2T_{BI} - T_B > T_W$, there is a time ratio of $\frac{T_B + T_W - T_{BI}}{T_{BI}}$ that the packet experiences double dangerous hops and a time ratio of $\frac{2T_{BI} - T_W - T_B}{T_{BI}}$ that the packet experiences single dangerous hop. Hence the successful probability of the packet not to be disturbed by a Bluetooth piconet is given by

$$P_s = \frac{T_W + T_B - T_{BI}}{T_{BI}} \times (57/79)^2 + \frac{2T_{BI} - T_W - T_B}{T_{BI}} \times (57/79) \qquad (3\text{-}11)$$

Case (iii)

From the above two cases, a similar form can be found in those P_s equations. If we substitute $T_{BI} - T_B - T_W$ with G in Case (i), we can obtain

$$P_s = (1 - \frac{|G|}{T_{BI}}) \times (57/79) + \frac{|G|}{T_{BI}} \times (57/79)^2 \quad (T_{BI} - T_B < T_W, \text{ i.e. } G < 0) \qquad (3\text{-}12)$$

and

$$P_s = (1 - \frac{|G|}{T_{BI}}) \times (57/79) + \frac{|G|}{T_{BI}} \times (57/79)^0 \quad (T_{BI} - T_B > T_W, \text{ i.e. } G > 0) \qquad (3\text{-}13)$$

If we substitute $2T_{BI} - T_B - T_W$ with G in Case (ii), we can obtain

$$P_s = (1-\frac{|G|}{T_{BI}}) \times (57/79)^2 + \frac{|G|}{T_{BI}} \times (57/79)^3 \qquad (2T_{BI} - T_B < T_W, \text{ i.e. } G < 0) \tag{3-14}$$

and

$$P_s = (1-\frac{|G|}{T_{BI}}) \times (57/79)^2 + \frac{|G|}{T_{BI}} \times (57/79) \qquad (2T_{BI} - T_B > T_W, \text{ i.e. } G > 0) \tag{3-15}$$

Observing equations (3-12) to (3-15), we see that the expressions for G and P_s have the same form. Thus we can extend this analysis to any length of T_W and T_{BI}. Let $G = \lceil T_W / T_{BI} \rceil \times T_{BI} - T_W - T_B$. The exponents of $(57/79)$ could be $\lceil T_W / T_{BI} \rceil - 1$, $\lceil T_W / T_{BI} \rceil$ or $\lceil T_W / T_{BI} \rceil + 1$. Therefore we obtain the general equation for P_s:

- When $\lceil T_W / T_{BI} \rceil \times T_{BI} - T_B < T_W$, the successful probability of the packet not to be disturbed by a Bluetooth piconet is given by

$$P_s = (1-\frac{|G|}{T_{BI}}) \times (57/79)^{\lceil T_W / T_{BI} \rceil} + \frac{|G|}{T_{BI}} \times (57/79)^{\lceil T_W / T_{BI} \rceil + 1} \tag{3-16}$$

$$(\lceil T_W / T_{BI} \rceil \times T_{BI} - T_B < T_W, \text{ i.e. } G < 0)$$

- When $\lceil T_W / T_{BI} \rceil \times T_{BI} - T_B > T_W$, the successful probability of the packet not to be disturbed by a Bluetooth piconet is given by

$$P_s = (1-\frac{|G|}{T_{BI}}) \times (57/79)^{\lceil T_W / T_{BI} \rceil} + \frac{|G|}{T_{BI}} \times (57/79)^{\lceil T_W / T_{BI} \rceil - 1} \tag{3-17}$$

$$(\lceil T_W / T_{BI} \rceil \times T_{BI} - T_B > T_W, \text{ i.e. } G > 0)$$

Equations (3-16) and (3-17) can be further combined as:

$$P_s = (1-\frac{|G|}{T_{BI}}) \times (57/79)^{\left\lceil \frac{T_W}{T_{BI}} \right\rceil} + \frac{|G|}{T_{BI}} \times (57/79)^{\left\lceil \frac{T_W}{T_{BI}} \right\rceil - \frac{G}{|G|}} \tag{3-18}$$

Consider an example: say $T_W = 2.3T_{BI}$. Then $\lceil T_W / T_{BI} \rceil$ is 3, so $G = 3T_{BI} - T_B - T_W$ and the exponents are 1, 2 or 3. We can therefore obtain P_s for the case of $2T_{BI} < T_W \leq 3T_{BI}$.

If there are N Bluetooth piconets in the neighborhood of the 802.11b network, the packet collision probability is given by

$$P_C = 1 - \left[(1 - \frac{|G|}{T_{BI}}) \times (57/79)^{\left\lceil \frac{T_W}{T_{BI}} \right\rceil} + \frac{|G|}{T_{BI}} \times (57/79)^{\left\lceil \frac{T_W}{T_{BI}} \right\rceil - \frac{G}{|G|}} \right]^N \quad (3\text{-}19)$$

Figure 3.16 shows the collision probability of an 802.11b packet in terms of different length of packet duration T_W in the presence of one Bluetooth piconet. T_B and T_{BI} have been given in Table 3.1 for different Bluetooth packet types. It is seen that 802.11b packets suffer the most from 1-slot Bluetooth packet, then from 3 and 5-slot packet in descending order. Since the use of multiple time slot packets effectively reduces the Bluetooth hop rate, thereby increasing the chances of successful reception of WLAN packets.

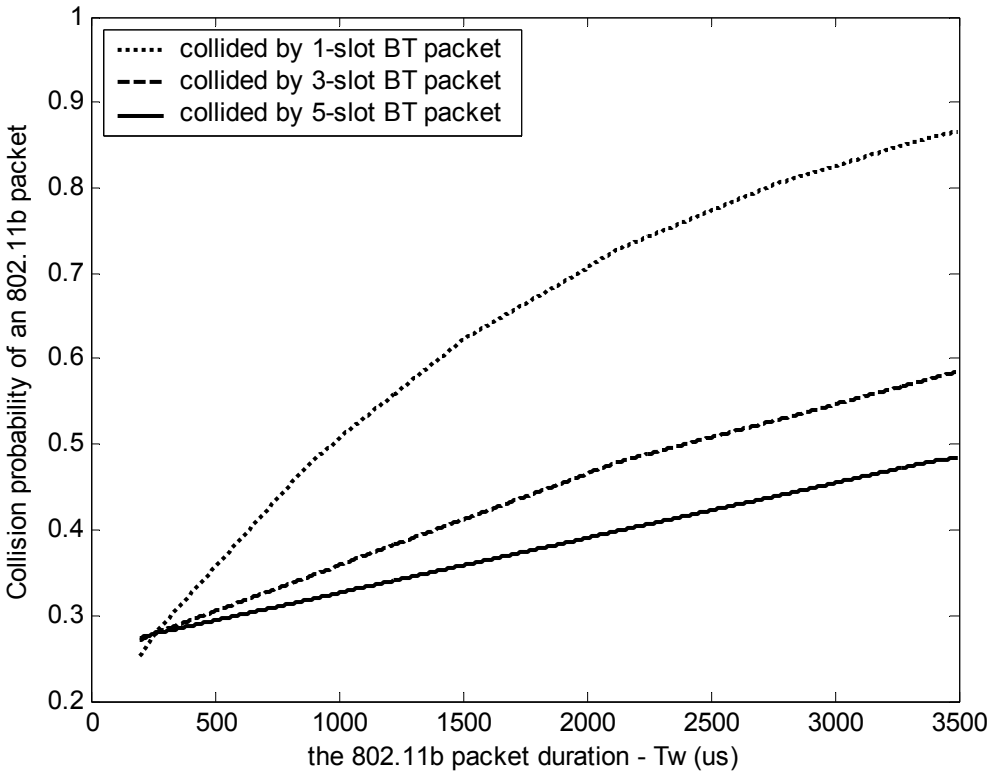

Figure 3.16 Collision probability of an 802.11b packet in the presence of one Bluetooth piconet

CHAPTER 4

PACKET ERROR RATE ANALYSIS IN BOTH PHY AND MAC LAYERS

In Chapter 2 and 3, BER and collision probability for both systems are analyzed in PHY and MAC layers respectively. The aim of this chapter is to analyze this problem in both PHY and MAC layers simultaneously, taking all transmission aspects (propagation effects, interference, thermal noise, modulation format and spread spectrum technique) into account. In this chapter, a metric of Packet Error Rate (PER) is introduced to give a more accurate model to analyze the systems performance. PER occurs when at least one bit is erroneously received in the packet. Bit error is detected at the receiver in the form of SNR or SIR that depends on the power transmitted, the distance traveled, and the path loss model used. The SNR or SIR then translates into a BER according to the modulation scheme and receiver implementation. Packet arrival rate and carrier channel selection is determined in MAC layer. A collision occurs when both the desired packet and the interfering packets overlap in time and frequency. This collision is detected at the receiver in the form of SIR too. However, as we know, the collision probability cannot be considered as the packet error probability unless the interference power is so strong to destroy the packet involved in collision.

In this chapter, we first present the propagation model for average power loss of a signal over an area as a function of distance; then followed by the interference model. We categorize the interference into white and colored noise, as well as co-channel and adjacent channel interference. The interference model solves the problem of how to

translate the interference into Eb/No form, and to be used in demodulation and error estimation at the receiver. The following packet definition for Bluetooth and 802.11b is to classify different packet types in the computation of the PER. Finally, the PER analysis according to various packet types is discussed for Bluetooth and 802.11b respectively.

4.1 Signal Propagation Model

In a wireless communication system, the transmitted signal is affected by a time and space varying channel, which introduces a plurality of channel impairments such as attenuation, multipath, linear distortion and noise in the desired signal. The power of the received signal is influenced mainly by two independent propagation phenomena, i.e., large scale fading and small scale fading. Large scale fading represents average power or path loss over a large area as a function of distance. This phenomenon is affected by prominent environment features such as office walls, floors, ceilings and fixtures. The statistics of large scale fading provides a way of computing estimated signal power or path loss as a function of distance. Small scale fading deals with large dynamic variations in the received signal amplitude and phase as a result of small changes in the spatial separation between the transmitter and receiver. Normally Bluetooth and 802.11b are deployed in office or home environment, thus slow or stationary movement is assumed for both systems. Therefore, we only consider flat and slow fading caused by multipath variation of signal and low Doppler spread. Channel model for small scale fading has been depicted in Chapter 2.

Large scale fading is a result of gross variations in the overall path between the transmitter and receiver. The pass loss written in the logarithmic scale is [65]

$$PL(d) = PL(d_0) + 10 \cdot n \cdot \log_{10}\left(\frac{d}{d_0}\right) \tag{4-1}$$

$PL(d_0)$ is the path loss at 1 meter from the transmitter. It is a function of the transmitter receiver heights, the carrier frequency, and the type of environment. It is given by [65]

$$PL(d_0) = 20\log\left(\frac{4\pi d_0}{\lambda}\right) = 40dB \tag{4-2}$$

where λ is a wavelength of 2.4 GHz wave and is equivalent to 12.5 cm, d_0 is 1 meter. For line-of-sight (LOS) situations the path loss exponent n is very close to the expected value for free-space propagation $n = 2$. The values for the path loss exponent found for LOS paths are within the range 1.8-2.0. For obstructed direct path (OBS) situations the path loss exponent value n can increases to 5 variously [42]. In this thesis, we adopt the path loss model of [64]:

$$PL(d)[dB] = \begin{cases} 40.2 + 20\log(d), & d \le 8m \\ 58.3 + 33\log(d/8), & d > 8m \end{cases} \tag{4-3}$$

where exponent $n = 2.0$ is selected for LOS situation ($d \le 8m$) and exponent $n = 3.3$ is selected for OBS situation ($d > 8m$). Note that this model does not directly account for multipath effects, although the path loss term beyond 8 meters does take into account some of the range reduction due to reflections. As with any empirical model, it represents mean path loss values. An estimated model such as the one used here is a highly useful tool for predicting performance that can be tied to average measurement.

In the Bluetooth specification, Bluetooth operating range is set to 10m, which is reasonable for a cable replacement. The transmit power is set to 1mW or 0 dBm. On the other hand, IEEE 802.11b operating range is designed for 100m, and the transmit

power is set to 100mW or 20 dBm. The path loss for Bluetooth is the same as that of an IEEE 802.11b radio signal since they both operate in the same frequency band and are deployed in a similar environment. Figure 4.1 represents the path loss for Bluetooth. Figure 4.2 shows the path loss for IEEE 802.11b. It is observed that 40 dB is lost in the first meter.

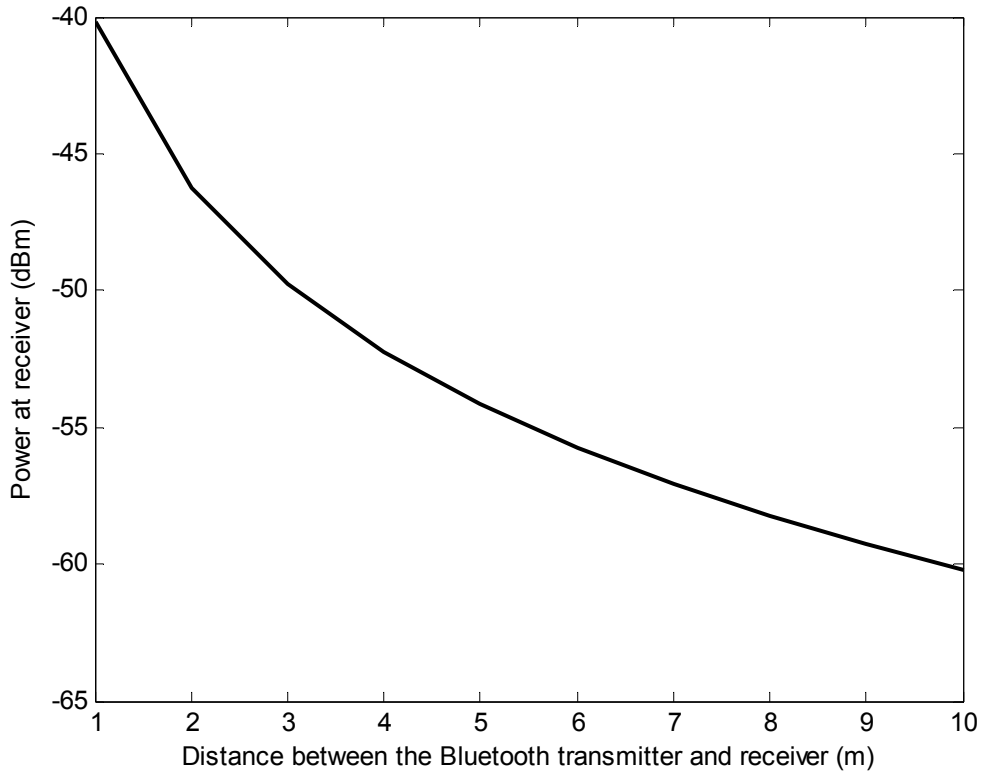

Figure 4.1 Path loss of Bluetooth in the wireless indoor channel

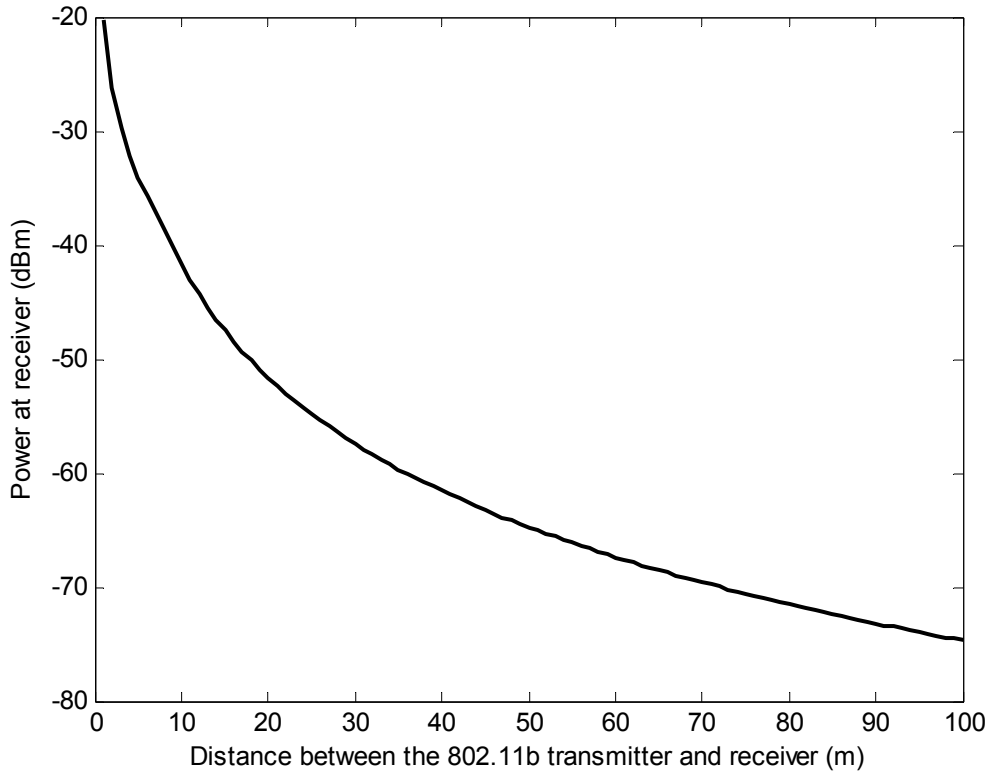

Figure 4.2 Path loss of 802.11b in the wireless indoor channel

4.2 Interference Model

4.2.1 White Noise

Successful operation of the system depends on the ability of a receiver to separate a desired signal from an undesired signal. This depends on the ratio between the energy of the desired signal and the total noise at the antenna of the receiver. This ratio is referred to as Eb/No (energy per bit over total noise) or SNR. The job of a receiver is to maximize the ability to decode desired signals from the noise. Noise can be categorized as either white or colored [63]. White noise generally describes wideband (i.e., wider than the desired signal) interference from multiple sources without any coordination between them. It can be modeled as a Gaussian random process where

successive samples of the process are statistically uncorrelated. Typically, the energy associated with white noise is distributed evenly across the frequency band and does not have any deterministic behavior over time or frequency. Thermal noise is considered as the Additive White Gaussian Noise (AWGN) and is determined by the product of Boltzman constant k, the environmental temperature ($T = 293K$) given in Kelvin Degrees and bandwidth of the system. The noise power spectral density is [68]

$$N_0 = k \cdot T \cdot BandWidth(1Hz) \cdot 10^3 mW \qquad (4\text{-}4)$$

Given the transmit powers of Bluetooth and 802.11b in addition to the path loss model, the Eb/No ratio under AWGN thermal noise can be obtained in terms of distance. A Bluetooth signal occupies a bandwidth of 1 MHz, so the value of N_0 is $4.02 \cdot 10^{-12} mW$; while for 802.11b, the baseband signal is spread to a bandwidth of 22 MHz, so the value of N_0 is $8.84 \cdot 10^{-11} mW$. E_b can be obtained by $P_t / PL(d)$; where P_t is transmit power of Bluetooth (0dBm) or 802.11b (20dBm); *PL(d)* is the path loss between the transmitter and the receiver. Eb/No of both systems under AWGN interference are shown in Figure 4.3 and Figure 4.4 respectively as a function of distance. It can be seen that if the systems only have interference from AWGN, Eb/No of each system is high enough for the receiver to correctly detect the desired signal within the defined operating range. Considering multipath effects, Eb/No could be much lower than this amount; but the value of Eb/No is still maintained for effective operation according to standards and specifications.

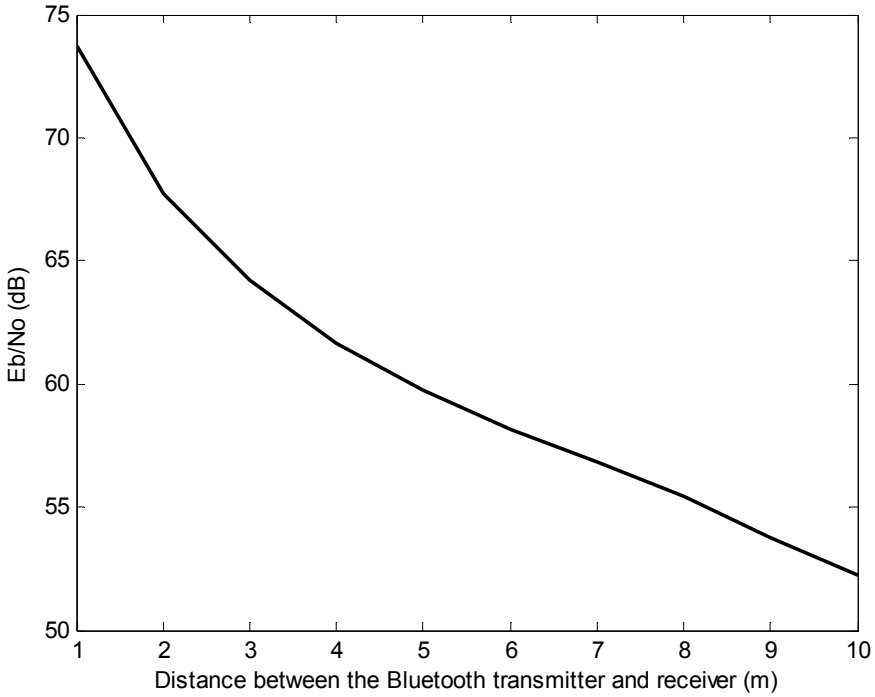

Figure 4.3 Eb/No of a Bluetooth signal with the distance

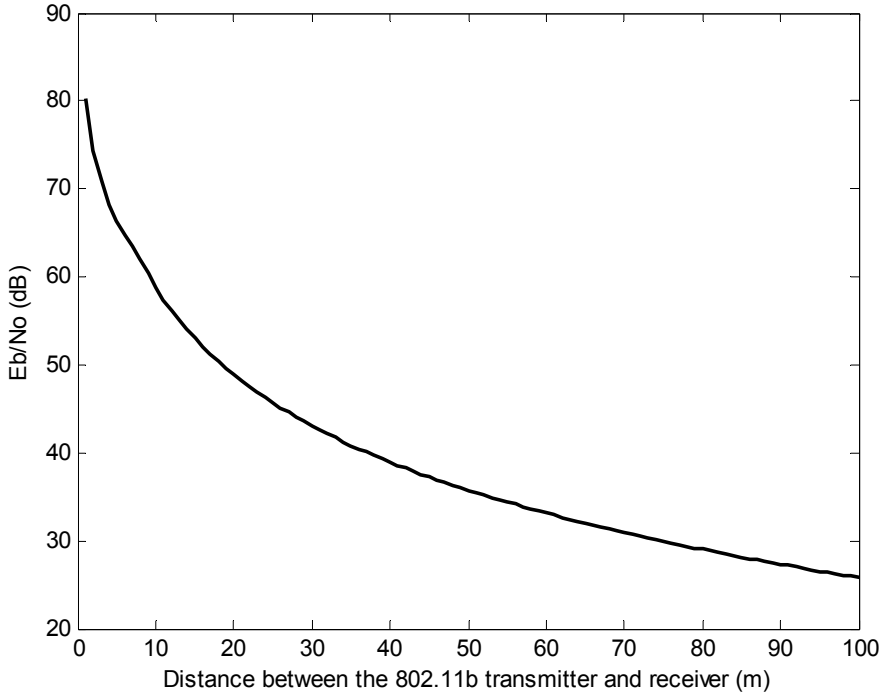

Figure 4.4 Eb/No of an 802.11b signal with the distance

4.2.2 Colored Noise

The second category of noise is colored noise. Colored noise is usually narrowband (i.e., relative to the desired signal) interference transmitted by intentional radio sets, and has a specific behavior in time and frequency. In case of a collision between the desired packet and the interfering packets, this collision is detected at the receiver in the form of SIR. Bluetooth radios create exactly the kind of colored noise. Now the problem is how to translate the interference on the signal into a BER form according to the carrier modulations and the receiver implementation used.

- **Co-channel Interference**

It is shown in [53] that the co-channel interference in angle modulation systems operating in slow Rayleigh fading has a Gaussian distribution. In [53], it is firstly proved that a single interferer at the output of the receiver filter is Gaussian noise. Then it is extended to multiple interferers. It is well known that the sum of jointly Gaussian random variables are Gaussian, and that independent Gaussian random variables are jointly Gaussian. Therefore, the sum of Gaussian interferes averaged across the slow Rayleigh fading is also Gaussian. In a Bluetooth system, coded bits are modulated using GFSK. For GFSK, information is conveyed by phase shifts relative to the previous signal interval. For example, the information bit 1 may be transmitted by shifting the phase of the carrier by $\pi/3$ relative to the previous carrier phase, whereas the information bit 0 is transmitted by a $-\pi/3$ relative to the phase in the preceding signaling interval. So at the *k*th signaling interval, a GFSK signal may be represented in complex-valued form as $S_k = \sqrt{E_s} e^{j(\theta_k - \phi)}$, where θ_k is the phase angle of the transmitted signal at the *k*th signaling interval, ϕ is the carrier phase. Thus, AWGN and interference can be added together to generate an equivalent Gaussian distributed noise.

Conversely, the transmitting signal of 802.11b interfering to the signal of Bluetooth is normally categorized as colored noise too. But IEEE 802.11b radio occupies a much wider band than Bluetooth, and thus can be assumed to appear as white noise to Bluetooth.

- **Adjacent Channel Interference**

Every transmitter is supposed to transmit only within a limited bandwidth; however, this is not physically possible without injecting noise to adjacent frequencies. The amount and nature of sideband signals created during transmission are determined by what is referred to as the transmitter's transmit mask. Sideband signals must be considered when evaluating interference between wireless systems sharing a frequency band [66,67]. In addition, receiver filters cannot be perfectly rectangular, meaning that the filter cannot precisely differentiate between signal and noise just inside and outside the passband. The combined impact of these transmitter and receiver masks explains what is referred to as adjacent channel interference. In our analysis, the adjacent channel interference is not considered. As we have depicted in GFSK modulation, a Gaussian filter is used to further reduce the side lobes of the transmitted baseband signal. As the bandwidth of the signal becomes narrower, the power in the side lobes of the transmitted signal, and consequently adjacent channel interference, reduces. We assume that out-of-band energy can usually be filtered out at the receiver, thus adjacent channel interference is ignored.

4.3 Packet Definition

4.3.1 Bluetooth

Bluetooth packets comprise three different fields (access code, header, and payload) in a fixed format (Figure 4.5). Each packet begins with a 72-bit access code for piconet identification and synchronization purpose. The access code is made up of three subfields: preamble (4 bits), trailer (4 bits), and Sync Word (64 bits); the last one is the only subfield sensitive to errors and is protected by a (64, 30) BCH code that can correct at most 9 errors [21]. A 54 bit header trails the access code determining the connected slave and other properties of the packet, and a payload of variable length. The header is protected by a simple three times repetition Forward-Error-Correction (FEC) code which can correct at most one error per codeword. The payload, depending on the considered packet type, can be protected or not by a (15, 10) shortened Hamming code, which can correct at most one error per codeword. A received access code is accepted if the number of matching bits in the 64 sync word bits of the access code exceeds a certain threshold. Header and bust payload are accepted if the respective header and payload cyclic-redundancy check (CRC) match. If any part fails, the packet has to be retransmitted.

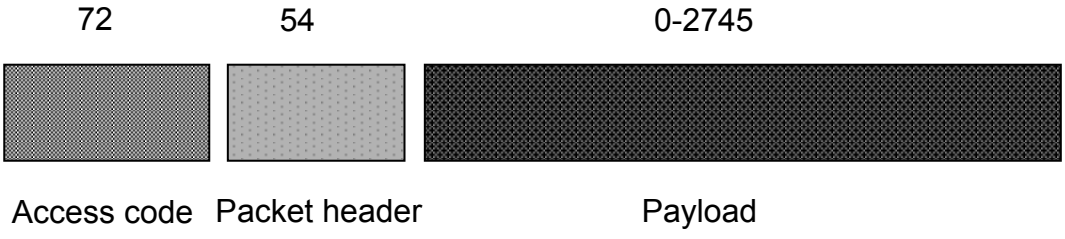

Figure 4.5 a Bluetooth packet format

Two types of links have been defined to support voice and data: Synchronous Connection-Oriented (SCO) link and, Asynchronous ConnectionLess (ACL) link.

SCO links support symmetrical, circuit-switched, point-to-point connections typically used for voice. These links are defined on the channel by reserving two consecutive slots (forward and return slots) with a fixed period. Reservation is carried out by the master and the slave when the link is setup. ACL links support symmetrical or asymmetrical, packet-switched, point-to-multipoint connections typically used for bursty data transmission. A set of packets has been defined for each physical link; the type of bits in the header indicates what packet is used. For SCO links, three kinds of single-slot voice packet (HV1, HV2 and HV3) have been defined, each of which carries voice at a rate of 64 kb/s. SCO bursts have no payload CRC and may therefore contain residual bit errors. For HV1 or HV2 type, a FEC rate of one-thirds or two-third can be selected; but for HV3 type, packet is sent unprotected. For ACL links, single-slot, 3-slot, and 5-slot data packets have been defined. Data can be sent either unprotected or protected by a two-thirds FEC rate. The maximum data rate – 723.2 kb/s in one direction and 57.6 kb/s in the reverse direction – is obtained from an unprotected, 5-slot packet. Figure 4.6 depicts mixed SCO and ACL links on a piconet with one master and two slaves. Slave 1 supports an ACL link and an SCO link with a 6-slot SCO period. Slave 2 only supports an ACL link. The SCO period can be decreased to 4-slot and 2-slot period. Thus three types of SCO link can occupy the whole, or half, or one-third capacity of a piconet.

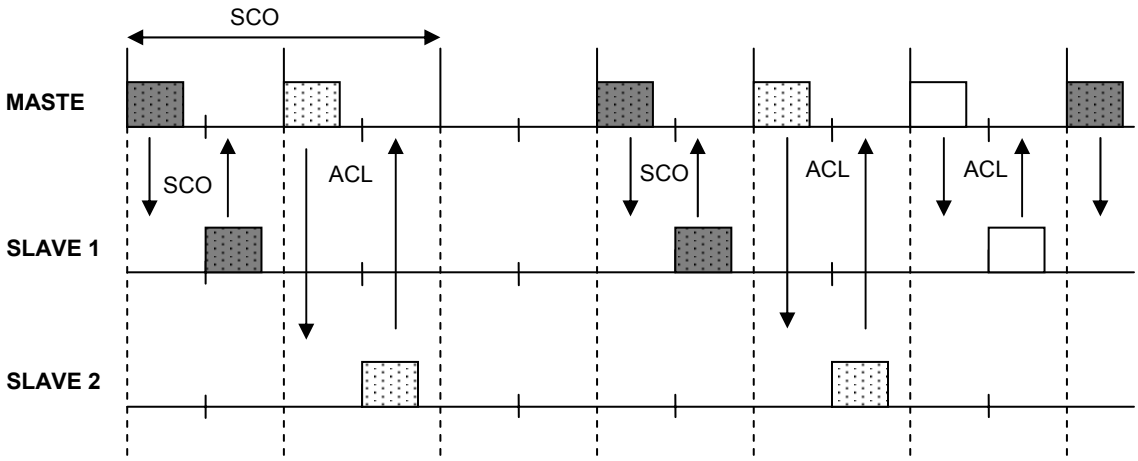

Figure 4.6 Example of SCO and ACL link mixing on a single piconet channel (each slot is on a different hop channel)

Table 4.1 shows some important properties of the available packet types for ACL and SCO. In DM packets, the payload is FEC coded with a simple 2/3 rate block code, while DH packet payloads are uncoded.

Table 4.1 Properties of Bluetooth Packet Types

Link Type	Packet Type	Playload FEC Code rate	User Payload (bytes)	Burst Length (μs)	Occupied Slots
Control	NULL		0	126	1
	POLL		0	126	1
ACL	DM1	2/3	0-17	171-366	1
	DM3	2/3	0-121	186-1626	3
	DM5	2/3	0-224	186-2871	5
	DH1	1	0-27	150-366	1
	DH3	1	0-183	158-1622	3
	DH5	1	0-339	158-2870	5
SCO	HV1	1/3	10	366	1
	HV2	2/3	20	366	1
	HV3	1	30	366	1

4.3.2 IEEE 802.11b

Each 802.11 MAC frame consists of three basic components [56]:

(1) A MAC *header*, which comprises frame control, duration, address, and sequence control information.

(2) A variable length *frame body*, which contains information specific to the frame type.

(3) A *frame check sequence*, which contains an IEEE 32-bit CRC.

Figure 4.7 depicts the general MAC frame format.

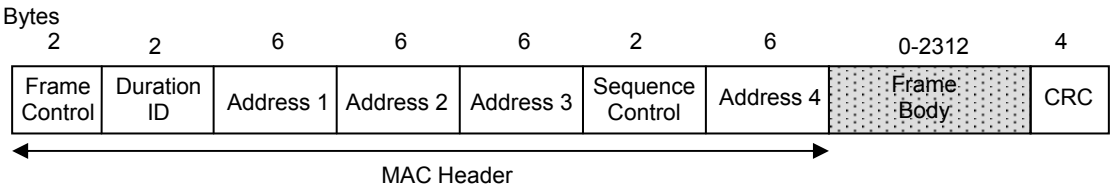

Figure 4.7 Standard IEEE 802.11 frame format

The preamble and header consists of five fields. They are: Preamble, SFD, Signal (rate), Service, Length and CRC. The preamble and header of the frame are always transmitted as the DBPSK waveform (1Mbps), while data packets can be configured for DBPSK, DQPSK or CCK. The duration of the preamble and the header is 192 μs. The Signal Field in the header of the packet indicates what modulation is used in the rest of the packet. The preamble is used by the receiver to achieve initial synchronization while the header includes the necessary data fields of the communications protocol to establish the physical layer link. The preamble and header are added to every packet transmitted on the LAN at the PHY layer of the system [56]. 802.11b packets are unprotected. Thus, when CRC detects that bit errors have occurred in the received packet, the packet needs to be retransmitted.

4.4 PER of Bluetooth

4.4.1 In the Presence of Bluetooth Piconets

Since multiple Bluetooth piconets are likely to coexist in a physical environment, the unrestricted access to the ISM frequency band exposes Bluetooth devices to encounter collisions inevitably.

We consider N piconets coexisting in a physically closed environment. Since no coordination is possible between piconets, each piconet has $N-1$ potential competitors. If two piconets transmit packets at the same time and frequency, collision occurs. The effect of collision on the packet is determined by the ratio of SINR that depends on the power transmitted, the distance traveled, and the path loss model used. The SINR then translates into a BER according to the GFSK carrier demodulation. An insufficient SINR at the receiver causes big probability of bit error. The SINR is given by the ratio of the received signal power to the total received interference power. The noise is thermal noise considered as AWGN with power spectral density of $\frac{N_0}{2} watts / hertz$.

The interference is attenuated by its path loss to the receiver and by the spectrum factor to account for the total interference power at the receiver. The interference power, hence the SINR, depends on the number of piconets as well as the distance from the desired receiver.

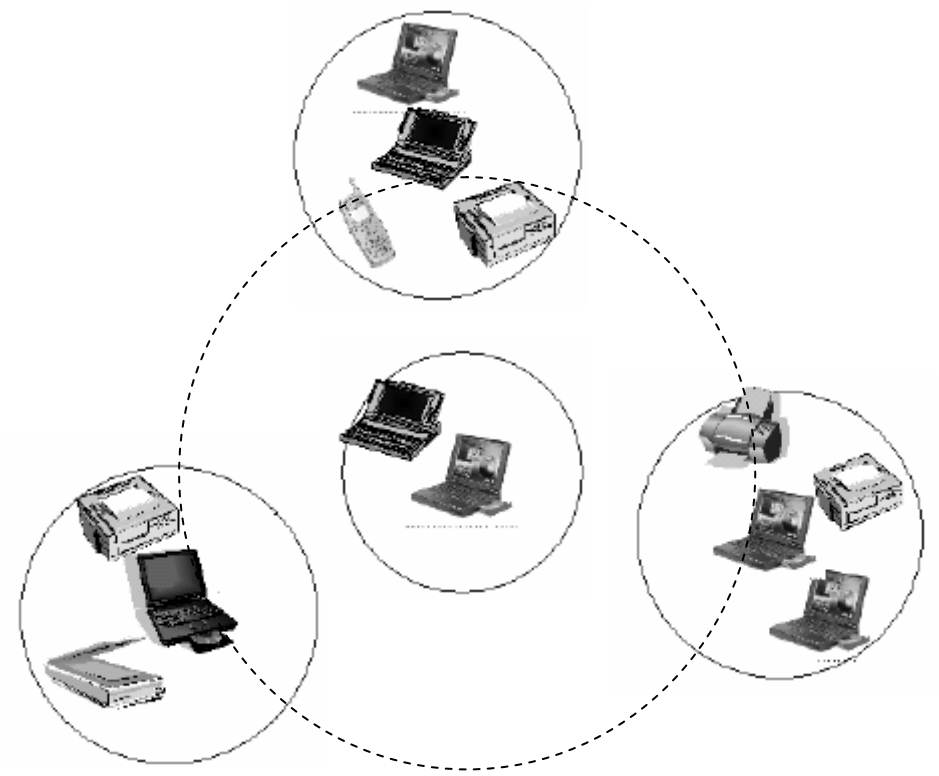

Figure 4.8 Considered interference scenario

The considered scenario, as shown in Figure 4.8, consists of a number of Bluetooth piconets assumed to be uniformly distributed in a circular region. Two Bluetooth devices working as a pair of transmitter and receiver are assumed to be placed in the center of the circular. Let us consider the desired piconet X and another competing piconet Y. The interference power at receiver X is $I_r = P_{t\_Y} / PL(d)$; where P_{t_Y} is the transmitted power of Y; *PL(d)* is the path loss between the transmitter Y and receiver X. The noise at the demodulator is filtered Gaussian noise with zero mean and variance $\sigma^2 = N_0 / 2$. The signal of Bluetooth occupies a bandwidth of 1 MHz, so N_0 is equal to $4.02 \cdot 10^{-12} mW$. As we have explained in a previous section, Bluetooth interference can be considered as Gaussian distributed noise approximately, thus the equivalent noise comprising AWGN and interference at the demodulator is filtered Gaussian noise with zero mean and variance $\sigma^2 = (N_0 + I_r)/2$. The information

signal power at receiver X is $P_r = P_{t\_X} / PL(d)$, where P_{t_X} is the transmitted power of X, P_r is the received power. Hence the SINR is $P_r /(N_0 + I_r)$. If there are n piconets colliding into the desired packet at the same time, the SINR therefore has the form of $P_r /(N_0 + n \cdot I_r)$.

A packet error is said to have occurred if at least one bit in the packet is received in error, so PER is given by $PER = 1-(1-P_e)^L$, where P_e is the error probability of a single bit, L is the number of bits in the packet. The analysis is exact under the assumptions that the signal bit error rate is constant throughout the duration of a packet. We assume that $P_e = 0$ if there is no collision. A Bluetooth packet is made up of three different fields, each one protected against errors by a different FEC block code. An accurate calculation of PER has to consider the error correction capabilities of the FEC codes adopted in the different fields, thus providing

$$PER = 1-(1-PE_{ac})(1-PE_{he})(1-PE_{pa}) \tag{4-5}$$

where PE_{ac} is the access code's word error probability; PE_{he} is the header code's word error probability; PE_{pa} is the payload code's word error probability. In the simulation of [21], results showed that the payload code's word error probability is approximately equal to the whole packet error probability. Hence,

$$PER \approx 1-(1-P_e)^{bits \quad in \quad payload} \tag{4-6}$$

The payload fields of six ACL packet types for which we wish to compute the PER are defined as follows [40]:

DM1: Occupies 1 forward slot. Payload consists of a 1 byte payload header, up to 17 bytes of data, and 16bit CRC, all of which are protected by the (15,10) Hamming code resulting in a maximum of 240 code bits.

DH1: Also occupies 1 slot and contains 240 total bits but is not protected by the Hamming code. The payload consists of a 1 byte header, 27 bytes of data, and 16 bit CRC.

DM3: Occupies 3 slots. Payload consists of a 2 byte payload header, 121 data bytes, and 16 bit CRC. The payload is protected by the Hamming code resulting in 1500 code bits.

DH3: Also occupies 3 slots but is not FEC encoded. Payload consists of a 2 byte header, 183 bytes of data, and 16 bit CRC, resulting in a total of 1496 bits.

DM5: Occupies 5 slots. Payload consists of a 2 byte header, 224 data bytes, and 16 bit CRC. It is FEC encoded producing 2745 code bits.

DH5: Occupies 5 slots but is not FEC encoded. Payload contains 2 byte header, 339 data bytes, and 16 bit CRC, resulting in a total of 2744 bits.

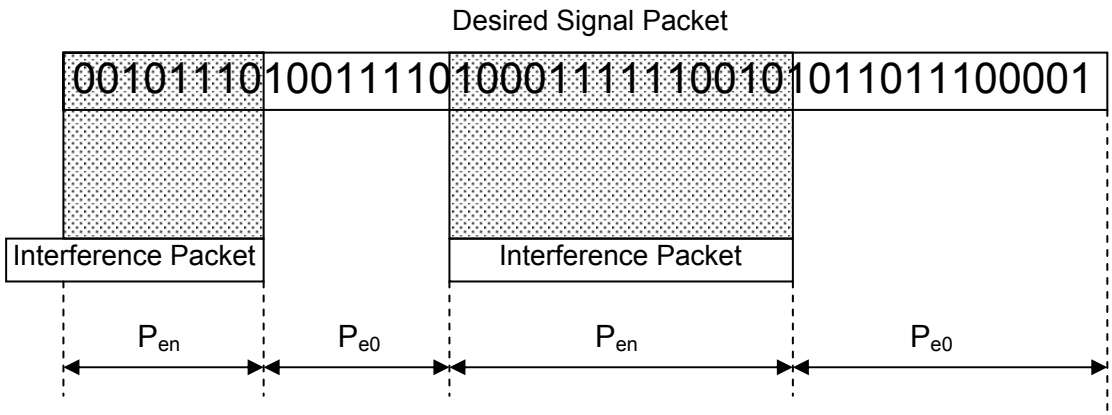

Figure 4.9 Packet collision and placement of errors

A collided packet has part of its bits overlapped by interference packet, as illustrated in Figure 4.9. Let us denote P_{e0} as the bit error probability for bits in the packet without collision; its SINR is $P_r/(N_0+0\cdot I_r)$. P_{e1} represents the bit error probability for bits in the packet overlapped by one packet; its SINR is $P_r/(N_0+1\cdot I_r)$; so on and so forth. P_r and I_r are obtained by using the adopted path loss formula in equation (4-3). BER is

calculated by substituting E_b / N_0 with $P_r /(N_0 + n \cdot I_r)$ in the lower bound BER formula for Bluetooth GFSK as given in equation (2-21).

In Bluetooth, 79 RF channels are equally visited. The probability that another packet hops into the desired packet's channel is $\frac{1}{79}$, the probability that this does not occur is $\frac{78}{79}$. We have discussed the collision probability of a Bluetooth packet in Section 3.3.1. Collision probability is computed if at least one bit in the packet is overlapped by other packets. As the calculation of PER is concerned with the total interference power, hence the number of interfering packets, we have to consider various collision situations separately. If there are $N-1$ potential interfering packets, there are N possible collision cases, listed as follows:

1. No packet from $N-1$ piconets collides into the desired packet,
   i.e. $P_c\{n=0\} = \left(\frac{78}{79}\right)^{N-1}$
2. Only one packet from $N-1$ piconets collides into the desired packet,
   i.e. $P_c\{n=1\} = C_{N-1}^{1}\left(\frac{1}{79}\right)\left(\frac{78}{79}\right)^{N-2}$
3. Only two packets from $N-1$ piconets collide into the desired packet,
   i.e. $P_c\{n=2\} = C_{N-1}^{2}\left(\frac{1}{79}\right)^{2}\left(\frac{78}{79}\right)^{N-3}$

   ⋮

N. All $N-1$ packets from $N-1$ piconets collide into the desired packet,
   i.e. $P_c\{n=N-1\} = \left(\frac{1}{79}\right)^{N-1}$

where C_y^x is defined as $\frac{y!}{(y-x)!x!}$.

In case of a collision with n piconets, the probability of a packet surviving the collision is $P_s(P_e \mid n)P_c\{n\}$, where $P_s(P_e \mid n) = (1-P_{en})^L$. n represents the total number of interfering packets that hops on the desired packet at the same time. As we suppose only part of the desired packet has been impacted and P_{en} is only used in the bits involved in overlapping, L considered here cannot be as long as the packet length. Assuming collision patterns are 100% uncorrelated, L should be an average value that takes all possible number of overlapped bits into consideration. Thus the average probability of a packet surviving from the collision is expressed as follows:

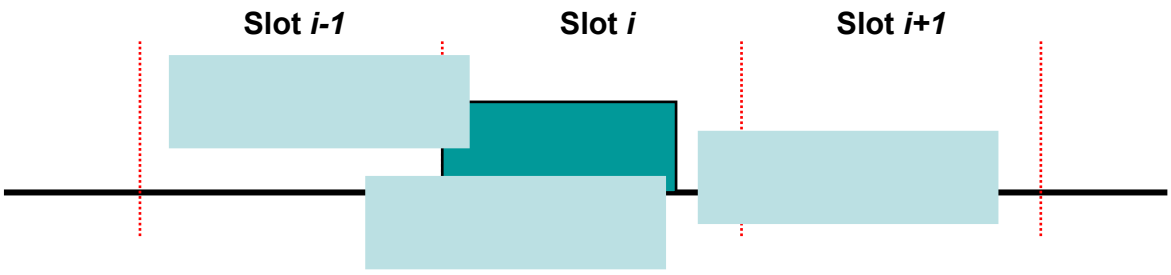

Figure 4.10 Collision placement of a 1-slot packet

DH1: DH1 is a single time slot packet and is the shortest packet type defined in Bluetooth. During the DH1 transmission time, each competing piconet only has time to generate one interfering packet at most. When a collision occurred, those interfering packets are from different competing piconets, and hopping positions are uncorrelated and independent. The interfering packets placement on the 1-slot packet is shown in Figure 4.10. So $P_s(P_e \mid n)$ is given by $P_s(P_e \mid n) = \frac{1}{625}\left[\sum_{k=1}^{366}(1-P_{en})^k + \sum_{k=367}^{625}(1-0)^k\right]$. The digit 366 represents the data

portion of the packet in bits; the digits 367 to 625 represent the idle time of the packet in bits.

The probability of a packet surviving in $N-1$ multi-Bluetooth environment is the summation of the packet's probability of survival under all collision cases. Thus P_s is given by:

$$P_s = P_s(P_{e0} \mid n) \cdot P_c\{n=0\} + P_s(P_{e1} \mid n) P_c\{n=1\} + \ldots + P_s(P_{eN-1} \mid n) P_c\{n=N-1\} \quad (4\text{-}7)$$

$$PER = 1 - P_s \quad (4\text{-}8)$$

DH3: DH3 occupies 3 successive slots in the same frequency channel. During its transmission time, each competing piconet could have three 1-slot packets transmitted on the air. To delimit DH3 in three single slots, where each slot is the time that allows only one single-slot packet could be generated from the competing piconet, the DH3 will experience three times single-slot time long collision threat. Denote P_{S1} the probability of survival for the first slot duration, P_{S2} for the second slot duration, and P_{S3} for the third slot duration. Thus P_S is given by

$$P_S = P_{S1} \cdot P_{S2} \cdot P_{S3} \quad (4\text{-}9)$$

$P_s(P_e \mid n)$ for P_{S1} and P_{S2} is the same and is given by $P_s(P_e \mid n) = \frac{1}{625} \sum_{k=1}^{625} (1-P_{en})^k$.

The digit 625 is the data portion of the first and second slots in bits.

$P_s(P_e \mid n)$ for P_{S3} is given by $P_s(P_e \mid n) = \frac{1}{625} \left(\sum_{k=1}^{372} (1-P_{en})^k + \sum_{k=373}^{625} (1-0)^k \right)$. The digit 372 is the data portion of the last slot, and the digits 373 to 625 are the idle time of the last slot in bits.

If the competing piconets are using 3- or 5-slot packet types, the duration of DH3 transmission could allow each piconet to generate only one interfering packet. The DH3 packet, therefore, experiences one time 3-slot long collision threat. P_s is given by Eq. (4-7). $P_s(P_e \mid n)$ is given by $P_s(P_e \mid n) = \frac{1}{1875}\left[\sum_{k=1}^{1622}(1-P_{en})^k + \sum_{k=1623}^{1875}(1-0)^k\right]$. The digit 1622 is the data portion of the packet in bits; the digits 1623 to 1875 are the idle time of the packet in bits.

DH5: DH5 occupies 5 successive slots in the same frequency channel. During its transmission time, each competing piconet could have five 1-slot packets transmitted on the air. To delimit DH5 in five single slots, where each slot is the time that allows only one single-slot packet could be generated from the competing piconet, the DH5 will experience five times single-slot time long collision threat. Denote P_{S1}, P_{S2}, … P_{S5} the successful probability for the slots duration. Thus P_S is given by

$$P_S = P_{S1} \cdot P_{S2} \cdot P_{S3} \cdot P_{S4} \cdot P_{S5} \tag{4-10}$$

$P_s(P_e \mid n)$ for P_{S1} to P_{S4} is the same and is given by $P_s(P_e \mid n) = \frac{1}{625}\sum_{k=1}^{625}(1-P_{en})^k$.

$P_s(P_e \mid n)$ for P_{S5} is given by $P_s(P_e \mid n) = \frac{1}{625}\left(\sum_{k=1}^{370}(1-P_{en})^k + \sum_{k=371}^{625}(1-0)^k\right)$.

If the competing piconets are using 3-slot packet types, the duration of DH5 transmission could allow each piconet to transmit two interfering packets on the air. The DH5 packet, therefore, experiences one time 3-slot long collision threat, and one time 2-slot long collision threat. Denote P_{3S} and P_{2S} the successful

probability for the duration of the first 3 slots and the last 2 slots. Thus P_S is given by

$$P_S = P_{3S} \cdot P_{2S} \tag{4-11}$$

$P_s(P_e \mid n)$ for P_{3S} is given by $P_s(P_e \mid n) = \frac{1}{1875}\sum_{k=1}^{1875}(1-P_{en})^k$.

$P_s(P_e \mid n)$ for P_{2S} is given by $P_s(P_e \mid n) = \frac{1}{1875}\left(\sum_{k=1}^{995}(1-P_{en})^k + \sum_{k=996}^{1875}(1-0)^k\right)$.

If the competing piconets are using 5-slot packet types, the duration of DH5 transmission could allow each piconet to generate only one interfering packet. The DH5 packet, therefore, experiences one time 5-slot long collision threat. $P_s(P_e \mid n)$ is given by $P_s(P_e \mid n) = \frac{1}{3125}\left[\sum_{k=1}^{2870}(1-P_{en})^k + \sum_{k=2871}^{3125}(1-0)^k\right]$.

In order to research the relationship between PER and the number of interfering piconets, hence to make the SINR only change with the number of piconets, the distance from interferer to the receiver is fixed at 5m; and the distance between the transmitter and the receiver is fixed at 2m. Depending on the different number of interferers, BER changes from 0.044 to 0.435. PER performances for DH1 to DH5 are shown in Figure 4.11, 4.12 and 4.13. Comparing with the collision probability obtained in section 3.3.1, PER is obviously smaller.

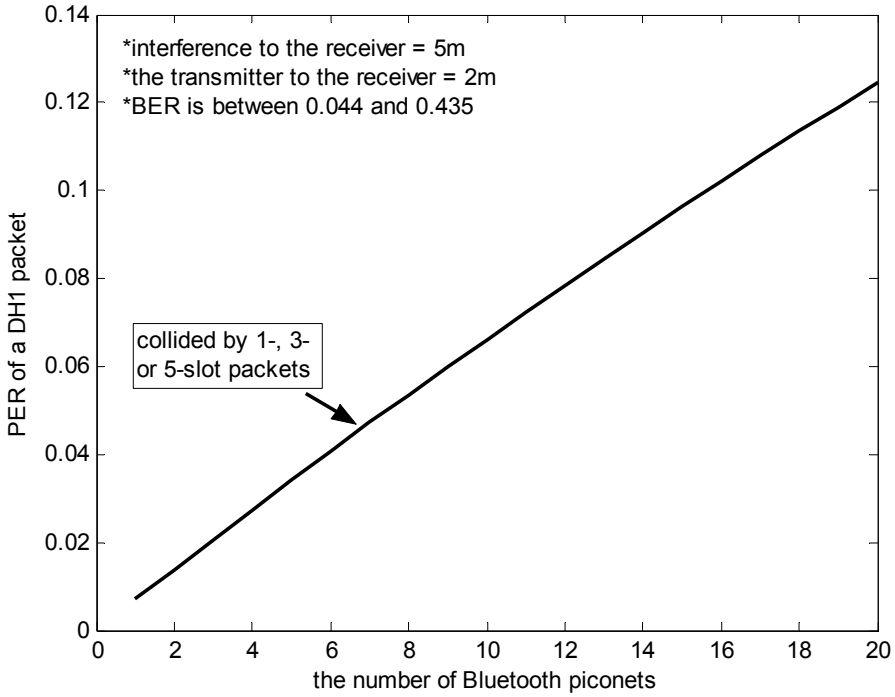

Figure 4.11 PER of a DH1 packet in the presence of multiple piconets

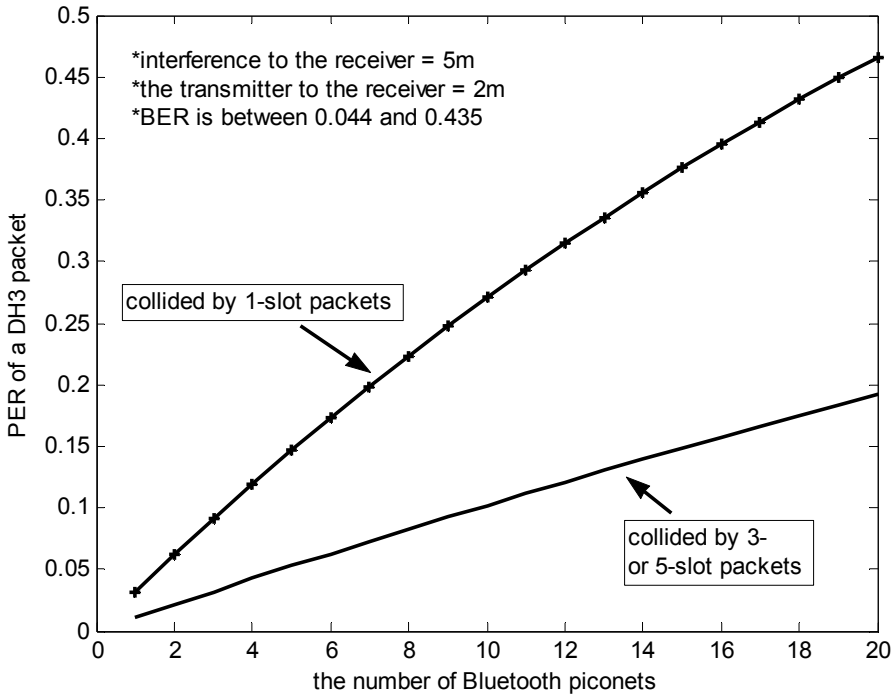

Figure 4.12 PER of a DH3 packet in the presence of multiple piconets

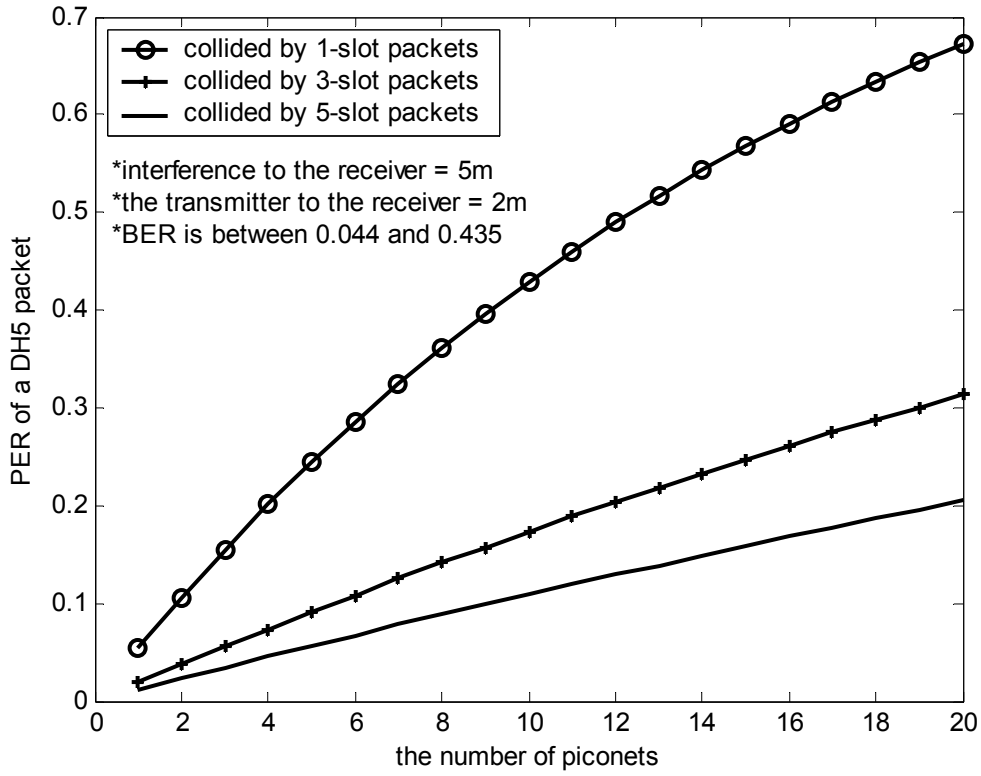

Figure 4.13 PER of a DH5 packet in the presence of multiple piconets

The payload of DMx packets is protected by a (15, 10) Hamming code, which is capable of correcting one bit error per 15 bit code block. The payload is correctly decoded provided that all code blocks contain one or no error, i.e. the probability of survival is given by [40]

$$P_{block} = 15 \cdot P_e \cdot (1 - P_e)^{14} + (1 - P_e)^{15} \tag{4-12}$$

The metric we use in the analysis of DMx packet includes the packet loss P_{LOSS}, and the packet error. The packet loss is the number of packets discarded due to uncorrected errors in the packet (after applying error correction effects of FEC); while the packet error is the number of packets received with at least one error (prior to applying error correction on the packet and deciding whether to keep it or drop it). However, it is hard to compute the accurate number of overlapping bits L caused by collision.

Hence, the method used in DHx PER computations cannot be used in the computation of P_{LOSS} of DMx packets directly. An alternative method could be found to evaluate the performance of DMx in the presence of interference. It is known that FEC can enhance the performance of packet error rate under the same interference condition. The simulation results shown in Figure 4.14 presents a ratio of PER without FEC to P_{LOSS} with a (15, 10) Hamming code. This figure shows that the (15, 10) Hamming code only helps to reduce the PER under low BER conditions. For BER lower than 0.01, PER performs 15 times worse than P_{LOSS}. However, when BER reaches to 0.05, the advantage of using this Hamming code is decreased. Furthermore, when BER reaches to 0.2, the performance of P_{LOSS} and PER is no difference.

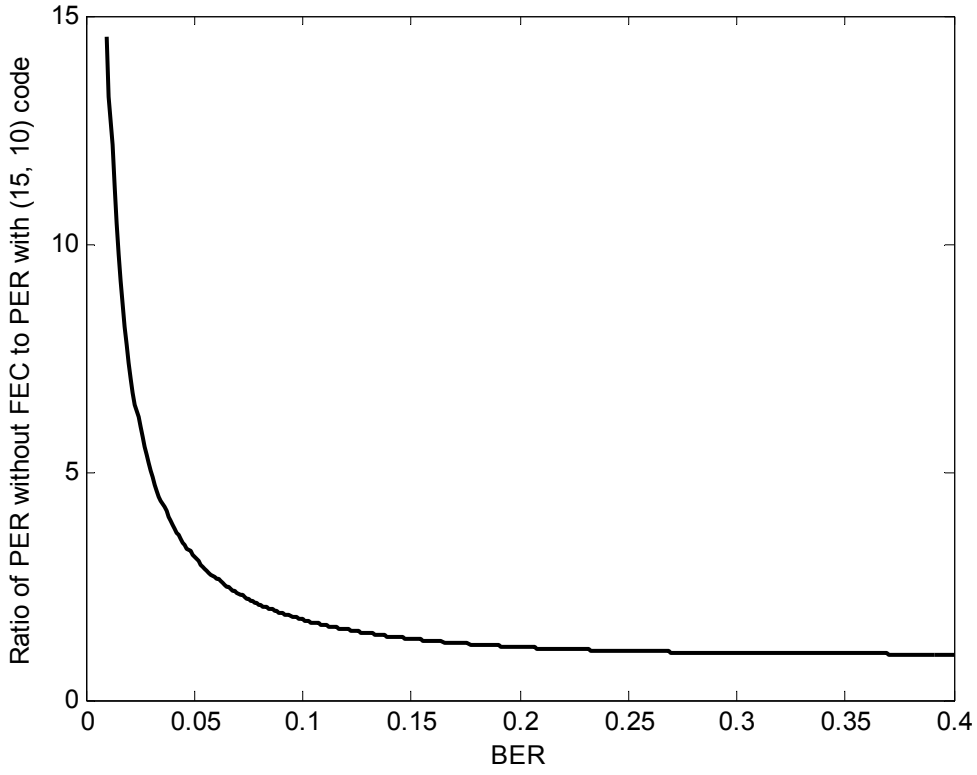

Figure 4.14 Performance comparisons between PER and packet loss

We found the BER in our considered scenario fall between 0.044 and 0.435 for different number of piconets in close proximity. The rate that DMx outperforms DHx under the same interference condition is shown in Figure 4.15. The horizontal axis is labeled as the number of piconets, which represents the same effect of BER. This consideration is to help us compare the performance between DHx and DMx in our scenario. From Figure 4.15, DMx packets only outperform DHx packets in the presence of less than two competing piconets. We can see using FEC in the Bluetooth payload does not improve performance a lot because the errors caused by interference are often too many to correct. This conclusion is consistent with the results of Zurbes [1][30] and Golmie [19]. The FEC algorithm of Bluetooth only works well with random errors which are distributed over the whole packet, instead of a burst of several consecutive errors, which is the case of packet collision.

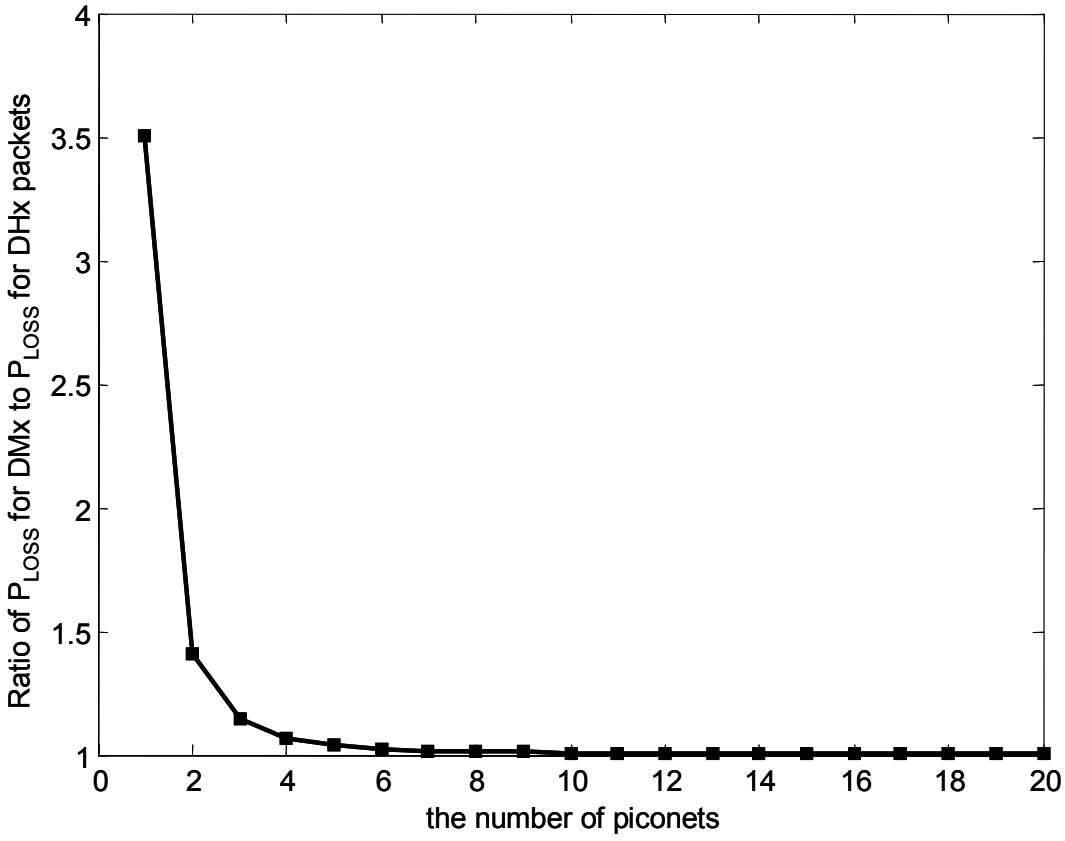

Figure 4.15 Performance comparison between DMx and DHx

4.4.2 In the Presence of 802.11b

As an 802.11b WLAN can cover an area of radius up to 100m, it is reasonable to assume that a Bluetooth piconet is only interfered by one 802.11b network.

Suppose the interfering signal power at receiver X is $I_r = \frac{P_{t\_Y}}{PL(d) \cdot 22}$; where P_{t_Y} is the transmitted power of an 802.11b station; *PL(d)* is the path loss between the 802.11b transmitter and receiver X; the digit 22 is the ratio of the 802.11b spread bandwidth to Bluetooth information bandwidth. Note that the powers are calculated after the spectrum factor has been applied, and so this ratio corresponds to the value after the receiver filter. The noise N_0 at the demodulator is equal to $4.02 \cdot 10^{-12} mW$. As we have previously explained, the 802.11b interference can be considered as Gaussian distributed noise approximately. Thus, the equivalent noise comprising AWGN and interference at the demodulator is filtered Gaussian noise with zero mean and variance $\sigma^2 = (N_0 + I_r)/2$. The information signal power at receiver X is $P_r = P_{t\_X} / PL(d)$, where P_{t_X} is the transmitted power of X, P_r is the received power. Hence the SINR is $P_r /(N_0 + I_r)$. BER is calculated by substituting E_b / N_0 with $P_r /(N_0 + I_r)$ in the Bluetooth BER formula (Eq. 2-21).

The probability of the packet received without error is given by

$$P_s = P_s(P_e \mid c)P_c + P_s(P_e \mid \bar{c})(1 - P_c) \qquad (4\text{-}13)$$

The first term of the equation describes the probability that a Bluetooth packet to be error free after collision with an 802.11b packet. The second term is the probability of the packet being error free without collision. Collision probability P_c is given in Eq. (3-

7), Subsection 3.3.2. Similarly, we assume $P_e = 0$ if there is no collision, which results in $P_s(P_e \mid \bar{c}) = 1$, and the average $P_s(P_e \mid c)$ has the following form:

DH1: $P_S(P_e \mid c) = \frac{1}{366}\left[\sum_{k=1}^{366}(1-P_{ec})^k\right]$

DH3: $P_S(P_e \mid c) = \frac{1}{1622}\left[\sum_{k=1}^{1622}(1-P_{ec})^k\right]$

DH5: $P_S(P_e \mid c) = \frac{1}{2870}\left(\sum_{k=1}^{2870}(1-P_{ec})^k\right)$

In the simulation, the distance from interferer to the receiver is fixed at 12m and the distance between the transmitter and receiver is fixed at 2m to generate a BER of 0.0035. PER performances in the presence of one 802.11b network for DH1, DH3 and DH5 are shown in Figure 4.16. Comparing with the collision probability obtained in Section 3.3.2, PER is obviously smaller.

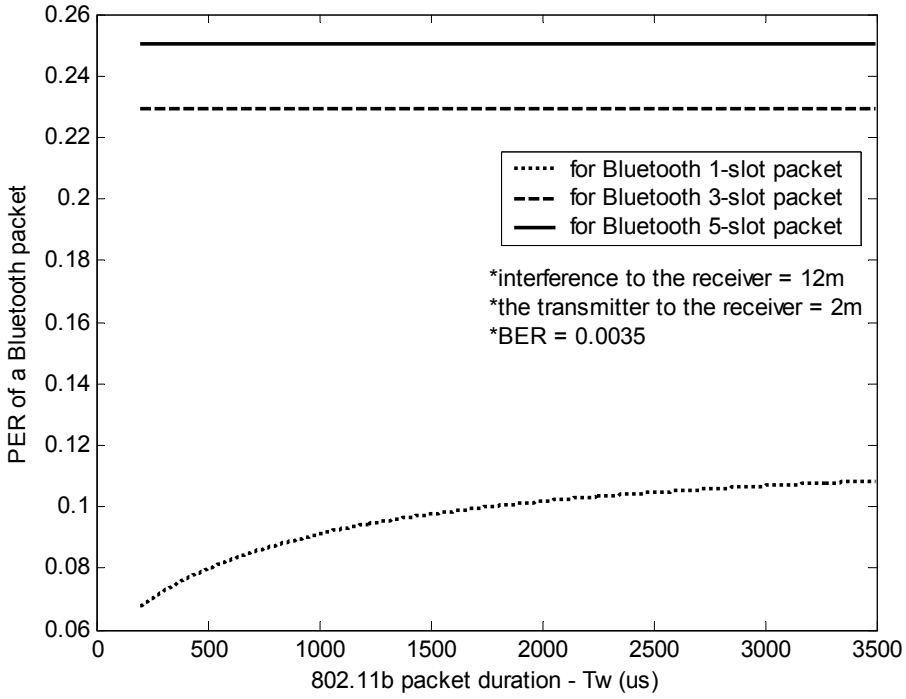

Figure 4.16 PER of a Bluetooth packet in the presence of 802.11b network

4.5 PER of 802.11b

According to the FCC regulations (FCC 15.247) for operation in the 2.4GHz ISM band the nominal power of the transmitter is 100mW or 20dBm. This signal strength was chosen to accommodate coverage of the approximately 100-meter radius area and to limit the battery power consumption. In such large range, a number of Bluetooth piconets are likely formed during the WLAN stations operation. We consider N piconets coexisting with an 802.11b WLAN in a physically closed environment.

The considered scenario consists of a number of Bluetooth piconets assumed to be uniformly distributed in a circular region. Two 802.11b stations working as a pair of transmitter and receiver, and the receiver is assumed to be placed in the center of the circular region. Let us consider the 802.11b receiver X and an interfering piconet Y. The interference power at receiver X is $I_r = P_{t\_Y} / PL(d)$; where P_{t_Y} is the transmitted power of Y; *PL(d)* is the path loss between transmitter Y and receiver X. If there are n piconets colliding with the desired signal at the same time, the total interference power is $I_b = n \cdot I_r$. The information signal power at receiver X is $P_r = P_{t\_X} / PL(d)$, where P_{t_X} is the transmitted power of X. The spread spectrum technique is employed in the IEEE 802.11b. The low power, spread signal is multiplied by the Barker code sequence at the receiver and returned to its original form, while the narrow band Bluetooth signal is spread to a relative wideband, thus resulting in the total interference power at the receiver divided by L_c, where L_c is the 802.11b spreading gain which we have explained in Section 2.5. As a transmitting signal of 802.11b occupies a bandwidth of 22 MHz, N_0 is equal to $8.84 \cdot 10^{-11} mW$. Note that the powers are calculated after the spectrum factor has been applied, and so this ratio corresponds to

the value after the receiver filter. SINR for four data rates of 802.11b are obtained from the considered model and summarized in Table 4.2.

Table 4.2 SNIR for 802.11b in the presence of Bluetooth piconets

data rate (Mbps)	spreading gain (L_c)	code gain (G_c)	SINR
1	11	--	$P_r/(N_0+\frac{I_b}{L_c})$
2	5.5	--	$\frac{P_r}{2}/(N_0+\frac{I_b}{L_c})$
5.5	2	1.53	$G_c\cdot\frac{P_r}{5.5}/(N_0+\frac{I_b}{L_c})$
11	1	1.53	$G_c\cdot\frac{P_r}{11}/(N_0+\frac{I_b}{L_c})$

Let us denote P_{e0} as the bit error probability for bits in a packet without collision; P_{e1} is the bit error probability for bits in a packet colliding with one piconet; so on and so forth. P_r and I_b are obtained by using the adopted path loss formula in equation (4-3). Substituting E_b/N_0 with SINR in Eq. (2-26), (2-27) and (2-34), we can obtain the BER of different 802.11b modulations under interference.

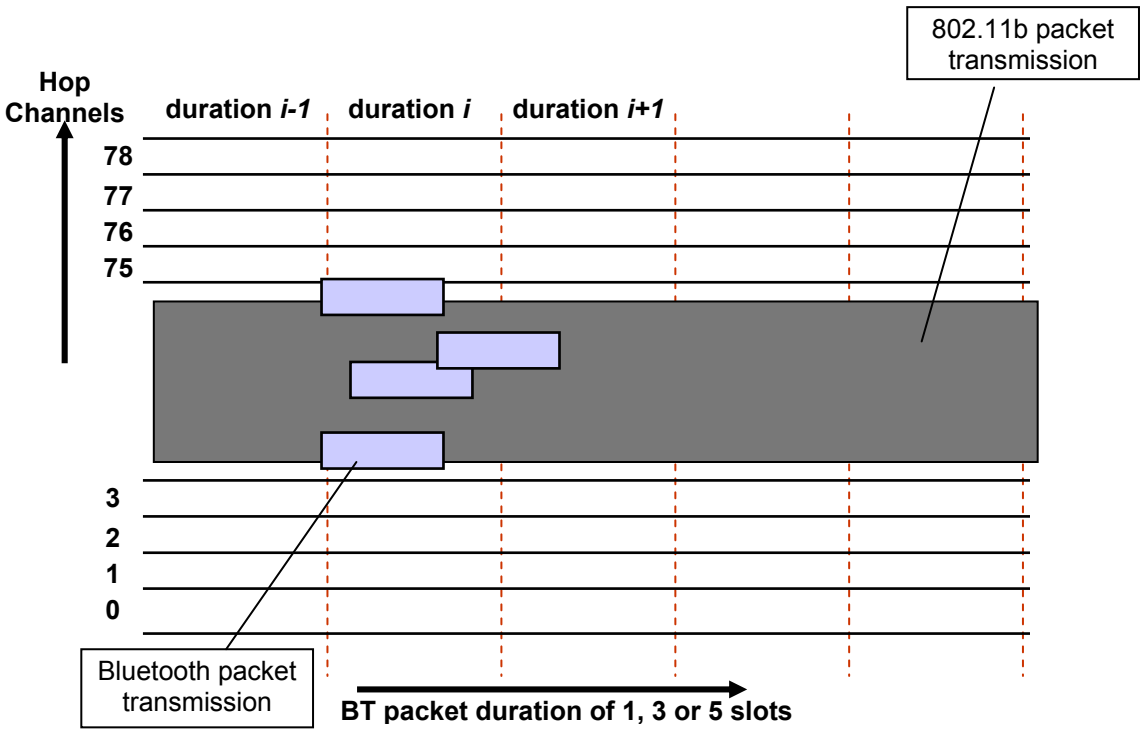

Figure 4.17 Diagram for the 802.11b packet collided by Bluetooth packets

In the analysis, the 802.11b packet is assumed to be sent asynchronously with respect to the Bluetooth packets, which use 1-, 3- or 5-slot types and have the same length packet each time. Transmission time of the desired packet is as long as a number of Bluetooth slots. As shown in Figure 4.17, we delimit an 802.11b packet transmission time into a number of Bluetooth packet durations. In each delimiter, the time allows N piconets only have N Bluetooth packets transmitting. A part of the N packets would hop on the 802.11b packet and cause diversity of collision patterns. The collision probability of an 802.11b packet in collision with a Bluetooth packet is 22/79, the probability that there is no collision is 57/79. As the calculation of PER is concerned with the total interference power, we have to know the number of interference packets for each collision pattern. The N interfering packets can lead to $N+1$ possible collision cases that the *i-th* delimiter would experience, which are listed below:

1. No packet from N piconets collides into the desired packet,

   i.e. $P_c\{n=0\} = \left(\frac{57}{79}\right)^N$

2. Only one packet from N piconets collides into the desired packet,

   i.e. $P_c\{n=1\} = C_N^1\left(\frac{22}{79}\right)\left(\frac{57}{79}\right)^{N-1}$

3. Only two packets from N piconets collide into the desired packet,

   i.e. $P_c\{n=2\} = C_N^2\left(\frac{22}{79}\right)^2\left(\frac{57}{79}\right)^{N-2}$

   ⋮

   ⋮

N+1. All N packets from N piconets collide into the desired packet,

   i.e. $P_c\{n=N\} = \left(\frac{22}{79}\right)^N$

where C_y^x is defined as $\frac{y!}{(y-x)!x!}$.

In case of collision, the probability of duration i surviving from the collision is $P_{Si}(P_e \mid n)P_c\{n\}$, where $P_{Si}(P_e \mid n) = (1-P_{en})^L$. n represents the number of the interfering packets. L is the number of bits involved in the impact. As we suppose only part of the desired packet has been impacted and P_{en} is only used in the bits involved in overlapping, L should be an average value that takes all possible number of overlapped bits into consideration. Thus the average probability of duration i surviving from the collision is in the form of $P_{Si}(P_e \mid n) = \frac{1}{L}\left(\sum_{k=1}^{L}(1-P_{en})^k\right)$. The probability of the *i-th* delimiter surviving in N multi-Bluetooth environment is the summation of the delimiter's probability of survival under all collision cases, where P_{Si} is given by:

$$P_{Si} = P_{Si}(P_{e0} \mid n) \cdot P_c\{n=0\} + P_{Si}(P_{e1} \mid n) P_c\{n=1) + \ldots + P_{Si}(P_{eN} \mid n) P_c\{n=N\} \quad (4\text{-}14)$$

The probability of the packet received without error can be written as $P_S = P_{S1} \cdot P_{S2} \cdot \ldots \cdot P_{SM}$, where $P_{S1/2/\ldots/M}$ is each delimiter successful probability, M is the number of consecutive Bluetooth packet transmission durations per 802.11b packet. Consequently, PER is given by

$$PER = 1 - P_S = 1 - P_{S1} \cdot P_{S2} \cdot \ldots \cdot P_{SM} \quad (4\text{-}15)$$

We plot the 802.11b PER performance according to this proposed analysis methodology via a Matlab simulation, and compare the results to the collision probability we obtained in Chapter 3. As 802.11b supports 4 data rates, we choose 1 Mbps mode in the simulation because it represents 1 bit per microsecond, just identical to Bluetooth, and it is easy to convert the packet duration in time to bits. First, let us see different length of 802.11b packet affected by one Bluetooth piconet. In the simulation, the distance from interferer to the receiver is fixed at 5m; the distance between the transmitter and receiver is fixed at 30m, which generates a BER of 0.003. We study the collision of three types of Bluetooth packets with an 802.11b packet. Its PER performance in the presence of one Bluetooth piconet is shown in Figure 4.18. Compare to its collision probability, PER is significantly smaller. This proves that the collision does not necessarily cause destruction of the packet, but the interference power does. Comparing the curves we obtained from two methodologies, the methods proposed for analysis the collision probability and the PER are in agreement. Note that the curves have some undulations which occur close to the integral divisors of a Bluetooth packet length. This reflects that the proposed PER calculation is discrete rather than continuous, and the minor bits remain in the last delimiter forces an additional collision danger.

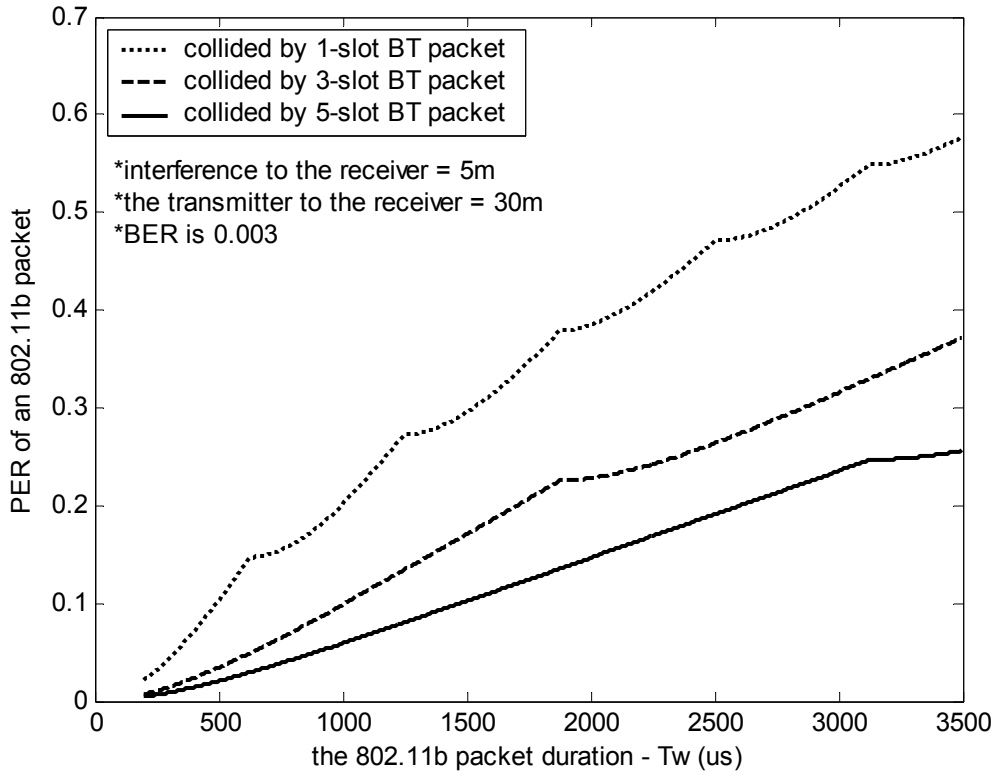

Figure 4.18 PER of an 802.11b packet in the presence of one Bluetooth piconet

Then let us see an 802.11b packet of fixed length affected by multiple Bluetooth piconets. Suppose the packet is 3000 μs long; the distance from interferers to the receiver is fixed at 5m; the distance between the transmitter and the receiver is fixed at 30m. BER is changing with the number of piconets. PER performance in the presence of multiple piconets is shown in Figure 4.19. It is easily observed that 802.11b packets are affected much more from Bluetooth, than Bluetooth suffers from 802.11b.

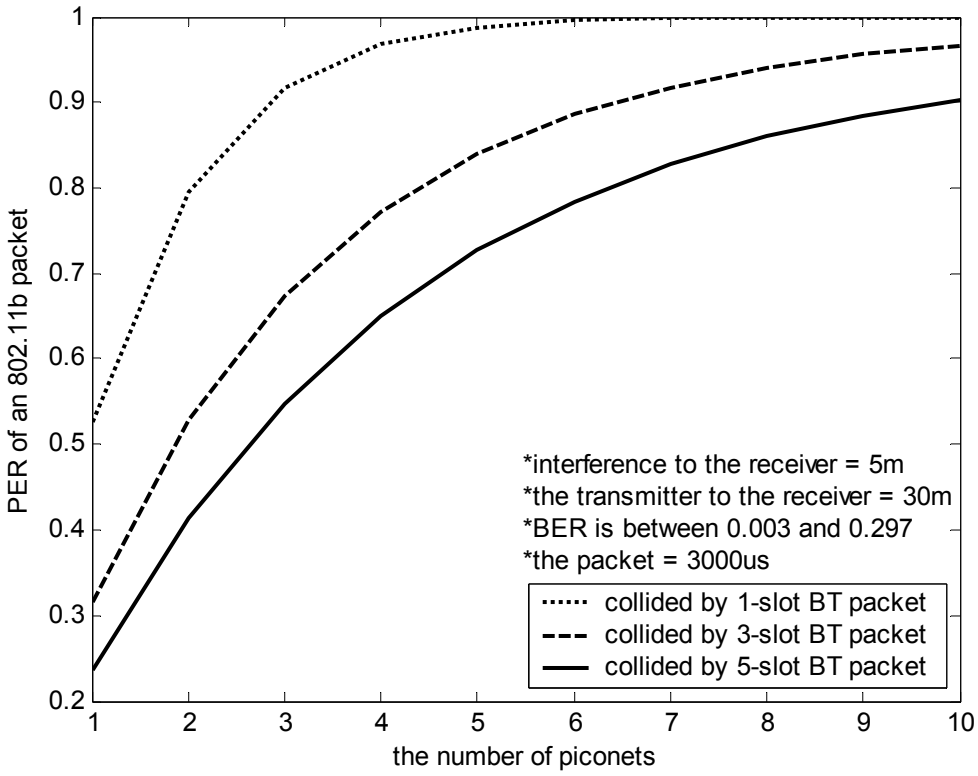

Figure 4.19 PER of an 802.11b packet in the presence of multiple Bluetooth piconets

CHAPTER 5

COEXISTENCE OF BLUETOOTH AND 802.11b NETWORK

In this chapter, we try to explain non-collaborative solutions for the coexistence problem. Our analysis is based on the fact that some parameters defined in the MAC and PHY layers can be selected and adjusted. We discuss how to select the optimal packet types, operating distance, packet size and data rate to enhance the system performance in a certain interference environment. This situation leads us to study how to optimize system throughput in a band with numerous, disparate, and uncoordinated interferers. A coexistence mechanism is implemented by selecting appropriate values of these parameters.

5.1 Throughput Calculation

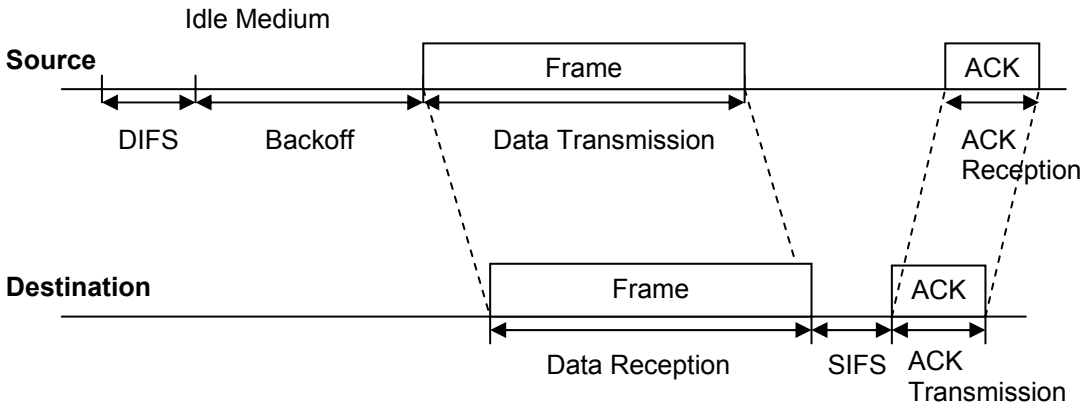

Figure 5.1 Average transmission scheme for 802.11b frame re-seize the medium

We have developed an appropriate model for analyzing the two systems' mutual interference in Chapter 2 to 4. It is found that a low PER is obtained at the expense of small data length, which, however, increases the transmission overhead. Under high SNR conditions, multi-slot packets or longer packets can improve system throughput. Thus the PER and packet length are conflicting goals. To balance them, the concept of throughput is used to optimize performance of the two systems. Throughput is defined as the average fraction of transmitted information that is successfully received over the radio channel in each second. The IEEE 802.11 MAC incorporates automatic repeat request (ARQ) to ensure reliable delivery of data across the wireless link. So there is little chance that the data will be lost. The effect that has on the WLAN is that those transmitted packets in failure need to be resent again, and the network latency increases, thus cause longer transmission time average for each packet. Recall that when an IEEE 802.11b frame arrives at the PHY layer, it will be attached the Physical Layer Convergence Protocol (PLCP) header and preamble. The PLCP overhead takes 192 μs in total. If the transmitting station detects that the wireless medium has been idle during a time interval DIFS, the station can transmit the frame immediately. For each successful reception of a frame, the receiving station immediately acknowledges the transmitting station by sending an ACK frame. Thus a transmission cycle, as shown in Figure 5.1, is composed of the following phases that are repeated over time: (1) DIFS deferral phase; (2) backoff contention; (3) PLCP overhead transmission phase; (4) Data transmission phase; (5) SIFS deferral phase; and (6) ACK transmission phase. Consequently the duration to transmit a data frame is given by

$$t_T = DIFS + Overhead + \frac{Data}{Rate} + SIFS + ACK + T_{backoff} \tag{5-1}$$

where the average backoff time is given by $\overline{T}_{backoff} = \frac{CW_{\min}}{2} \cdot aSlotTime$ [31], *Data* is the data portion of the packet in bits, *Rate* is data rate.

The physical parameters of the 802.11b are summarized in Table 5.1.

Table 5.1. IEEE 802.11b PHY parameters

Parameter	**Value**
a Slot time	20μs
SIFS time	10μs
DIFS time	50μs
PLCP Preamble	144μs
PLCP Header	48μs
ACK	112μs
CW_{min} (slot times)	31
CW_{max} (slot times)	1023

According to the 802.11b MAC protocol, a Stop-and-Wait ARQ is implemented in our simulations. If the data transmission fails, the station has to wait for an ACK timeout period, execute a backoff and retransmit the frame. We assume there is no retry limit for each failing frame. We assume that only one-way transmission and the probability of a packet being received in error is *p*. Therefore the average transmission time for a single frame is given by [77]:

$$t_{av} = t_T + (1-p) \cdot \sum_{i=1}^{\infty} i \cdot p^i \cdot t_T = \frac{t_T}{1-p} \tag{5-2}$$

where

$$(1-p)\cdot\sum_{i=1}^{\infty} i\cdot p^i\cdot t_T = t_T\cdot p\cdot(1-p)\cdot\sum_{i=1}^{\infty} i\cdot p^{i-1}$$

$$= t_T\cdot p\cdot(1-p)\cdot\frac{d}{dp}\left[\sum_{i=1}^{\infty} p^i\right]$$

$$= t_T\cdot p\cdot(1-p)\frac{d}{dp}\left[\frac{p}{1-p}\right]$$

$$= \frac{t_T\cdot p}{1-p}$$

Hence, the throughput of 802.11b system is given by

$$Throughput(bits/\sec) = Data/t_{av} = Data\cdot(1-p)/t_T \tag{5-3}$$

where $Data$ is as previously defined, t_T is the time to transmit a data packet consisting of overhead and the data portion, p is the packet error probability. The ARQ employed in Bluetooth is based on a stop-and-wait scheme with a minimal wait period: one slot. The success or failure of a packet is directly revealed in the header of the return packet. Based on receiving ACK or NAK the transmitter can send a new payload or has to retransmit the previous payload. Thus the average transmission time for a Bluetooth is $\frac{t_T}{1-p}$, too. The throughput expression of Bluetooth system is common to Eq. (5-3). The time to transmit a Bluetooth data could be 625, 1875 and 3125 μs respectively for three type packets.

The aim of our proposed coexistence solution is to achieve graceful throughput degradation when the two systems operate in a shared environment.

5.2 Optimum Throughput for Bluetooth

5.2.1 In Multiple Piconets Environment

- Optimum packet type

Bluetooth packets have deterministic length and transmission time. Using throughput calculation, we can observe which packet type is optimum for a Bluetooth device in the presence of multiple piconets. The maximum raw throughput of Bluetooth DHx packet types is obtained according to Eq. (5-3), and the corresponding $Data$ and t_T are given in Table 5.2.

Table 5.2 The maximum raw throughput of DHx packet types

Packet type	Transmission time (t_T) (μs)	Max $Data$ (bits)	Max throughput (Kbits)
DH1	625	366	585.6
DH3	1875	1622	865
DH5	3125	2870	918.4

The interference distance can affect BER, hence PER, used in throughput calculation. However, we do not consider the effect of distance. We assume PER is equal to the collision probability, which corresponds to the worst case scenario. We believe the performance of different packet types have their own characteristics and results obtained under the assumption can indicate the general performance of them under whatever kind of condition. We are interested in the throughput performance in multiple Bluetooth piconets environment. In Figure 5.2, the throughput of three packet types is displayed as a function of the number of piconets, when it is interfered by 1-slot packets.

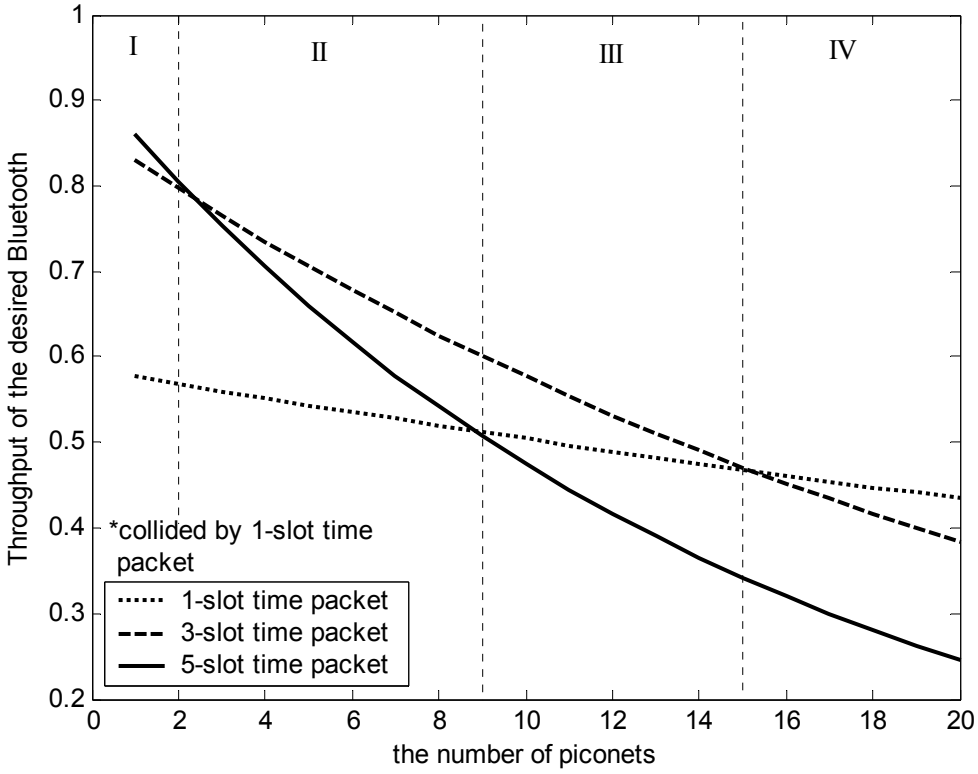

Figure 5.2 Throughput of a Bluetooth piconet suffered by 1-slot packets interference

The results show that 5-slot packet performs best in area I in Figure 5.2, if there are less than two piconets. The sequence from the best to the worse is 5, 3, and 1-slot packet. In area II, it is 3, 5, and 1-slot packet. In area III, the sequence is 3, 1, and 5-slot. If the number of piconets is more than 15, as we can see in area IV, 1-slot packet performs best, then 3-slot packet, the last 5-slot packet. Also we can conclude that 1-slot packet has good ability to combat the large number of potential interferers. However, long packet types such as 3 and 5-slot long are much more bandwidth-efficient than smaller ones. It is worth noting that the optimum packet types are selected based on throughput capacity rather than a certain throughput threshold. But the results also help to make decision based on performance threshold if it exists. The selection is that when the performance of a packet type degrades lower than its

threshold, the system chooses another packet type which can maintain relatively high throughput.

The throughput of three packet types when it is suffered from 3 and 5-slot packets is shown in Figure 5.3 and Figure 5.4 respectively.

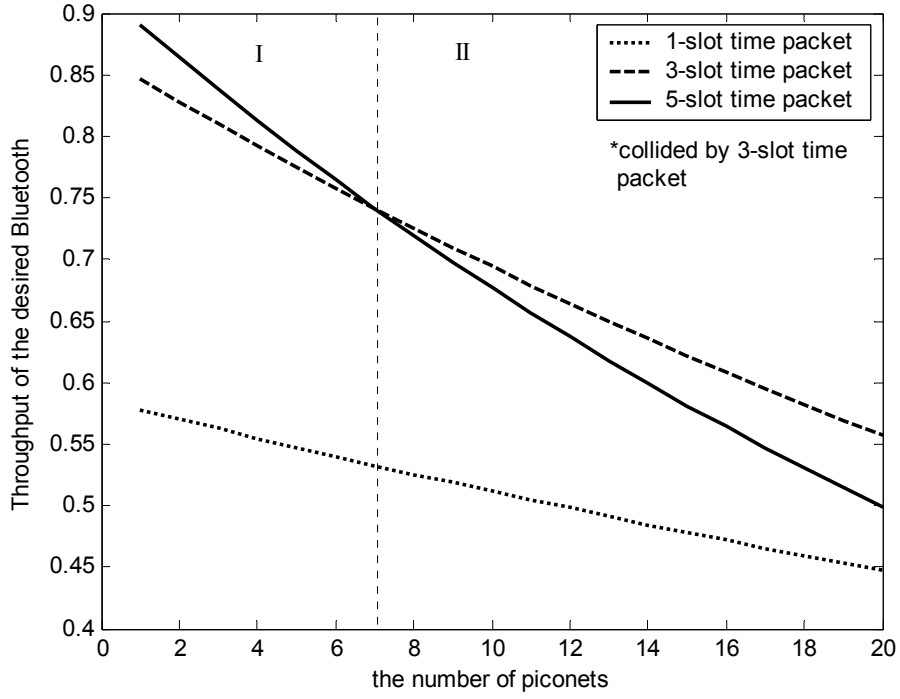

Figure 5.3 Throughput of a Bluetooth piconet suffered by 3-slot packets interference

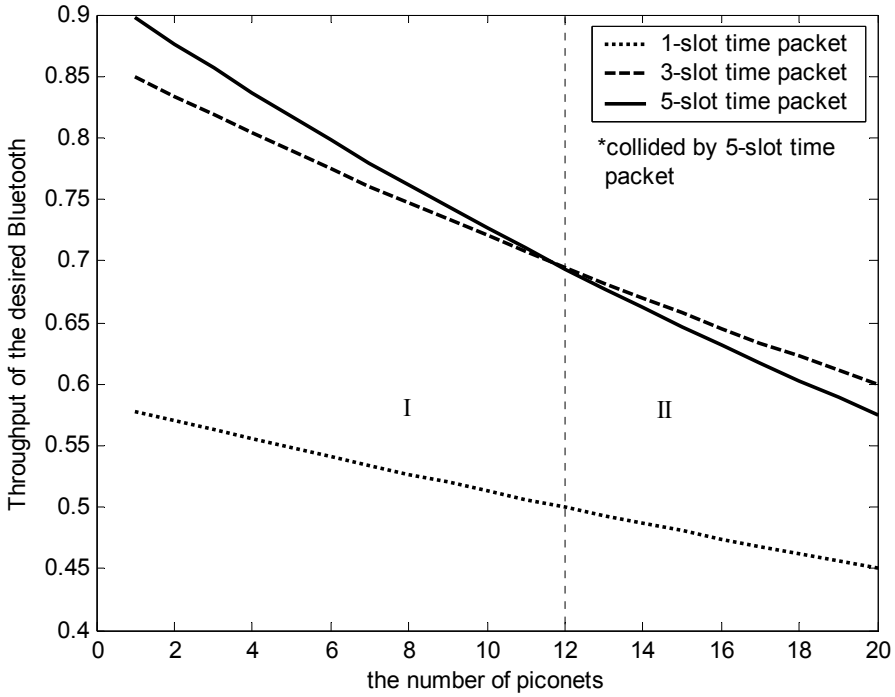

Figure 5.4 Throughput of a Bluetooth piconet suffered by 5-slot packets interference

To integrate these results, the optimum packet types selected for maximum throughput performance in an environment of high interference are summarized in Table 5.3 as well as the performance degradation percentage at performance interchange points.

Table 5.3 The optimum packet types for a Bluetooth in highly interfered environment

Simulation conditions	Rate packet types from best to worst			Interference conditions (interfering piconets)	Performance degradation (in sequence of 1, 3 & 5-packet types)		
When collided by 1-slot packets	5	3	1	< 2	3%	9%	14%
	3	5	1	Between 2 and 9	12%	30%	44%
	3	1	5	Between 9 and 15	20%	46%	63%
	1	3	5	> 15	25%	55%	73%
When collided by 3-slot packets	5	3	1	< 7	9%	14%	19%
	3	5	1	> 7	23%	35%	45%

When collided by 5-slot packets	5	3	1	< 12	14%	19%	24%
	3	5	1	> 12	23%	30%	37%

- Safe distance

In Bluetooth, a $C/I_{co-channel}$ of 11 dB is required for the detector to work efficiently. The signal and interference power at the receiver could be estimated as a function of distance by using a large scale fading model. We adopt the path loss formula as Eq. (4-3). Let d_u represent the distance between the desired transmitter and receiver; d_I represent the distance between the interfering transmitter and the receiver.

1. If both d_u and d_I are less than 8 m:

$$P_{r\_u} = P_{t\_u} - PL(d_u) = 0dBm - (40.2 + 20\log d_u)$$

$$P_{r\_I} = P_{t\_I} - PL(d_I) = 0dBm - (40.2 + 20\log d_I)$$

where P_{t_u} is the transmit power (0 dBm) of a signal; P_{r_u} is the received power of the signal; P_{t_I} is the transmit power (0 dBm) of an interferer; and P_{r_I} is the detected interference power of the receiver.

In Bluetooth, a co-channel protection ratio of 11 dB is required, i.e.

$$SIR = P_{r\_u} - P_{r\_I} = 20\log\left(\frac{d_I}{d_u}\right) = 11dB$$

Thus we obtain the distance ratio of $\frac{d_I}{d_u} = 3.5$.

2. If both d_u and d_I are larger than 8 m:

$$P_{r\_u} = P_{t\_u} - PL(d_u) = 0dBm - \left(58.3 + 33\log\left(\frac{d_u}{8}\right)\right)$$

$$P_{r\_I} = P_{t\_I} - PL(d_I) = 0dBm - \left(58.3 + 33\log\left(\frac{d_I}{8}\right)\right)$$

$$SIR = P_{r\_u} - P_{r\_I} = 33\log\left(\frac{d_I}{d_u}\right) = 11dB$$

Thus we obtain the distance ratio of $\frac{d_I}{d_u} = 2.1$.

3. If $d_u < 8m$ and $d_I > 8m$:

$$P_{r\_u} = P_{t\_u} - PL(d_u) = 0dBm - (40.2 + 20\log d_u)$$

$$P_{r\_I} = P_{t\_I} - PL(d_I) = 0dBm - \left(58.3 + 33\log\left(\frac{d_I}{8}\right)\right)$$

$$SIR = P_{r\_u} - P_{r\_I} = -11.7 + 33\log d_I - 20\log d_u = 11dB$$

Thus we obtain an approximate relationship between d_I and d_u, which is $d_I - d_u \geq 8m$.

5.2.2 In the Presence of 802.11b

- Optimum packet types

With the same consideration as Subsection 5.2.1, we do not consider the effect of distance in the procedure to find the optimum packet type of Bluetooth in the presence of 802.11b network. We assume PER is equal to the collision probability, which corresponds to the worst case scenario. The throughput of three packet types in the presence of an 802.11b network is shown in Figure 5.5. The interfering packet length of 802.11b is different. It is obviously found that different 802.11b packet sizes have

little effect on the throughput of 3 and 5-slot packet, where 5-slot packet has the best throughput performance. With 802.11b interference, the throughput of 5-slot packet degrades by 28%.

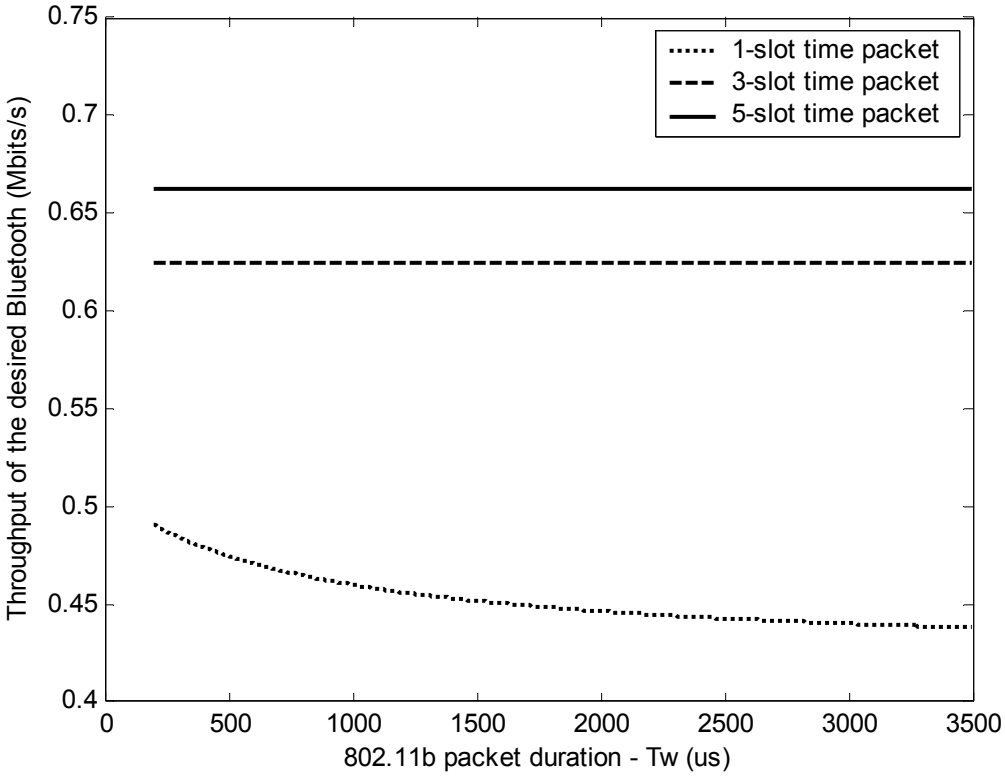

Figure 5.5 Throughput of a Bluetooth piconet in the presence of an 802.11b network

- Safe distance

Following is the calculation of the safe distance of Bluetooth to 802.11b transmitter.

1. If both d_u and d_I are less than 8 m:

$$P_{r\_u} = P_{t\_u} - PL(d_u) = 0dBm - (40.2 + 20\log d_u)$$

$$P_{r\_I} = P_{t\_I} - PL(d_I) = 20dBm - (40.2 + 20\log d_I) - 13.4dB$$

$$SIR = P_{r\_u} - P_{r\_I} = 20\log\left(\frac{d_I}{d_u}\right) - 6.6 = 11dB$$

13.4dB is spreading gain obtained from 802.11b because 802.11b signal is transmitted in much lower power in spread channel. Thus we obtain the distance ratio of $\frac{d_I}{d_u} = 7.6$.

2. If both d_u and d_I are larger than 8 m:

$$P_{r\_u} = P_{t\_u} - PL(d_u) = 0dBm - \left(58.3 + 33\log\left(\frac{d_u}{8}\right)\right)$$

$$P_{r\_I} = P_{t\_I} - PL(d_I) = 20dBm - \left(58.3 + 33\log\left(\frac{d_I}{8}\right)\right) - 13.4dB$$

$$SIR = P_{r\_u} - P_{r\_I} = 33\log\left(\frac{d_I}{d_u}\right) - 6.6 = 11dB$$

Thus we obtain the distance ratio of $\frac{d_I}{d_u} = 3.4$.

3. If $d_u < 8m$ and $d_I > 8m$:

$$P_{r\_u} = P_{t\_u} - PL(d_u) = 0dBm - (40.2 + 20\log d_u)$$

$$P_{r\_I} = P_{t\_I} - PL(d_I) = 20dBm - \left(58.3 + 33\log\left(\frac{d_I}{8}\right)\right) - 13.4dB$$

$$SIR = P_{r\_u} - P_{r\_I} = -18.3 + 33\log d_I - 20\log d_u = 11dB$$

Thus we obtain the relationship between d_I and d_u, which is listed in Table 5.4.

Table 5.4 safe distance difference between d_u and d_I

d_u (m)	1	2	3	4	5	6	7	8
d_I (m)	10	11	14	17	19	22	25	27
Distance difference ($d_I - d_u$)	9	9	11	13	14	16	18	19

5.3 Throughput of 802.11b

IEEE 802.11b defines four data rates. Each rate should have its optimal operating range to others. In this section, we first discuss the optimal ranges for 802.11b various data rates; then we analyze the safe distance ratio for an 802.11b receiver to Bluetooth interference. A packet segmentation measurement is proposed when an 802.11b receiver is operating within a dangerous distance to interferers. Last we discuss what the appropriate moment is for 802.11b system to scale higher rates down.

5.3.1 Efficiency Ranges for 802.11b Four Data Rates

Without considering multipath fading effects, we know the defined transmit power (20dBm) for an 802.11b transmitter can provide sufficient Quality of Service (QoS) for all applications. In order to let our results be close to a realistic situation, we set the Eb/No ratio to be 15 dB worse in the Rayleigh fading channel. The formula for the throughput generates the graph (Figure 5.6) for the throughput of four 802.11b data rates. From Figure 5.6, we can observe the efficiency of each rate versus distance. 11 Mbps gives the best throughput for the first 50 meters, then 5.5 Mbps performs the best for the next 15 meters, then 2 Mbps becomes more efficient for next 20 meters and finally 1Mbps gives the best throughput at 80 meters and beyond. As a result, we can see there is no single modulation that can be optimal under all scenarios. In general, the higher the transmission rate, the higher will be the SNR required to maintain the same communication quality, and as a result, the distance of transmission using the higher rates is less than that of the lower rates.

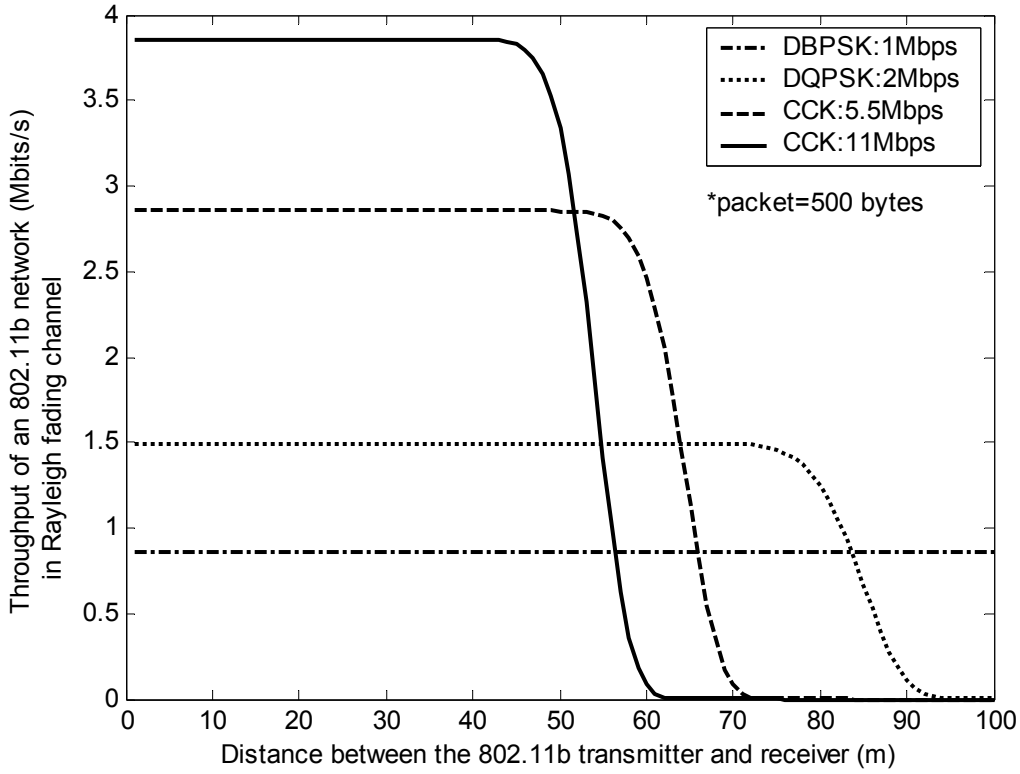

Figure 5.6 Optimal ranges for 802.11b four data rates

5.3.2 Safe Distance

In IEEE 802.11b, there is no requirement for co-channel protection ratio. The safe distance could be derived from PER performance in terms of distance. To reduce complexity, d_I and d_u use the same path loss model given by $PL(d) = 40.2 + 33\log(d)$. From the collision probability of 802.11b impacted by Bluetooth, we know when the two systems coexist in close proximity, Bluetooth should use long packets, like 5-slot packets. Thus when we discuss the safe distance ratio, we only consider the 802.11b packet is interfered by 5-slot packets; and the number of interferers is from one to three. Given a fixed packet size of 500 bytes, the receiver's performance of various data rates in the presence of one piconet is obtained and shown in Figure 5.7 in terms of PER.

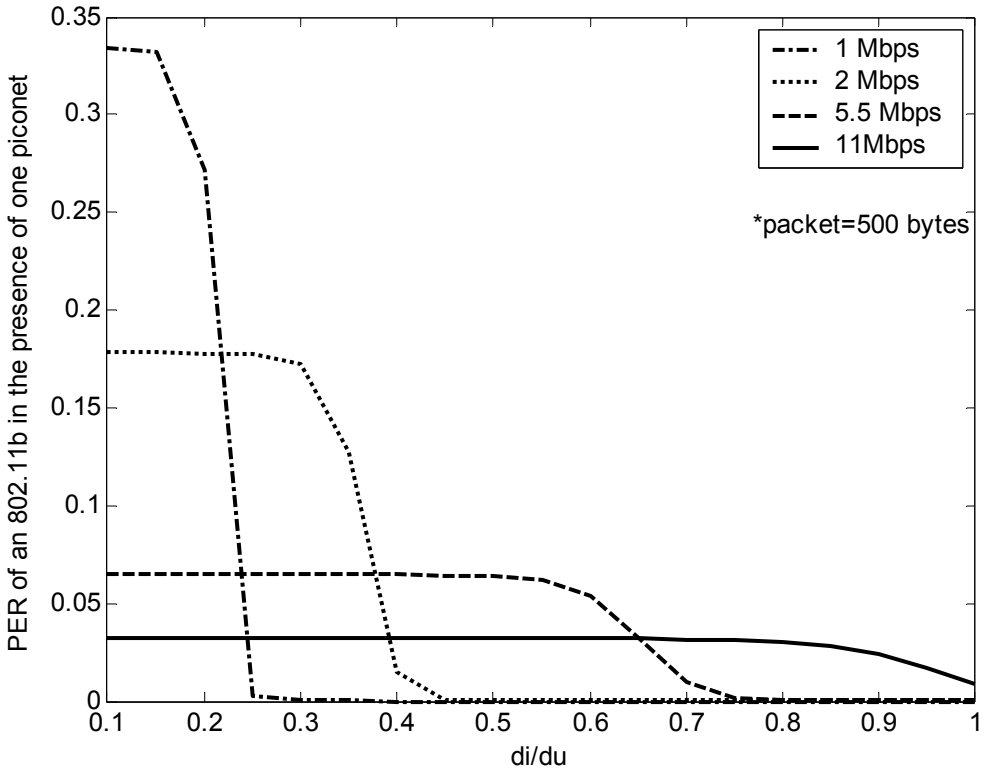

Figure 5.7 safe distance for an 802.11 receiver in the presence of one piconet

It can easily be observed that PER of each data rate reaches its maximum value and keeps stable when Bluetooth transmitters are very close. The effect results from that the interference power in a collision is so strong that error probability of the packet involved in collision equals one. In this situation, the *PER* is equal to the collision probability which is determined by packet transmission time T_W; but little relates to the distance. This explains why 1 Mbps mode has the highest error probability, followed by 2, 5.5 and 11 Mbps; because the transmission time in 1 Mbps mode is the longest. With increasing distance between interferer and the receiver, PER of 1 Mbps mode decreases sharply at the ratio of 0.25, followed by 2 Mbps, 5.5 Mbps and 11 Mbps at the ratio of 0.45, 0.75 and 1, respectively. The error rates are very low beyond these ratio points, thus they can be considered as safe distance ratios.

Increasing the number of Bluetooth piconets, the safe distance ratio increases as shown in Figure 5.8 and 5.9. We summarize safe distance ratios for 802.11b in the presence of Bluetooth in Table 5.5. From these results, it can be seen that lower data rates are able to operate closer to interference than higher data rates.

Table 5.5 Safe distance ratios for 802.11b in the presence of Bluetooth

	piconets=1				piconets=2				piconets=3			
Rates (Mbps)	1	2	5.5	11	1	2	5.5	11	1	2	5.5	11
Safe di/du	0.25	0.45	0.75	>1	0.3	0.5	0.85	>1	0.35	0.55	0.9	>1

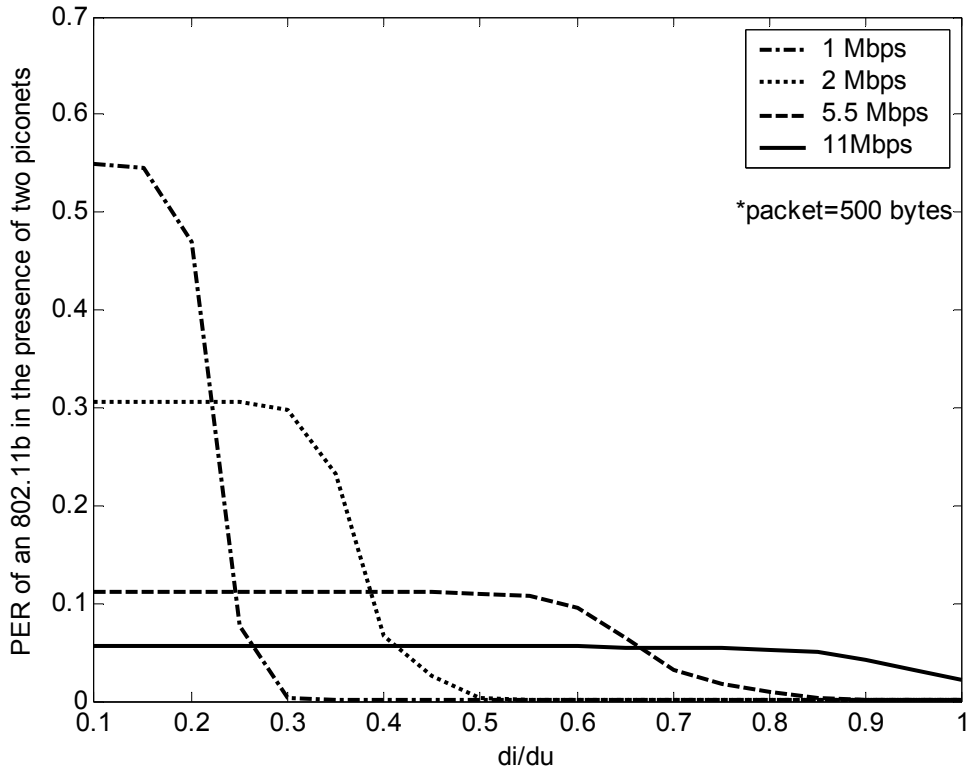

Figure 5.8 safe distance for an 802.11 receiver in the presence of two piconets

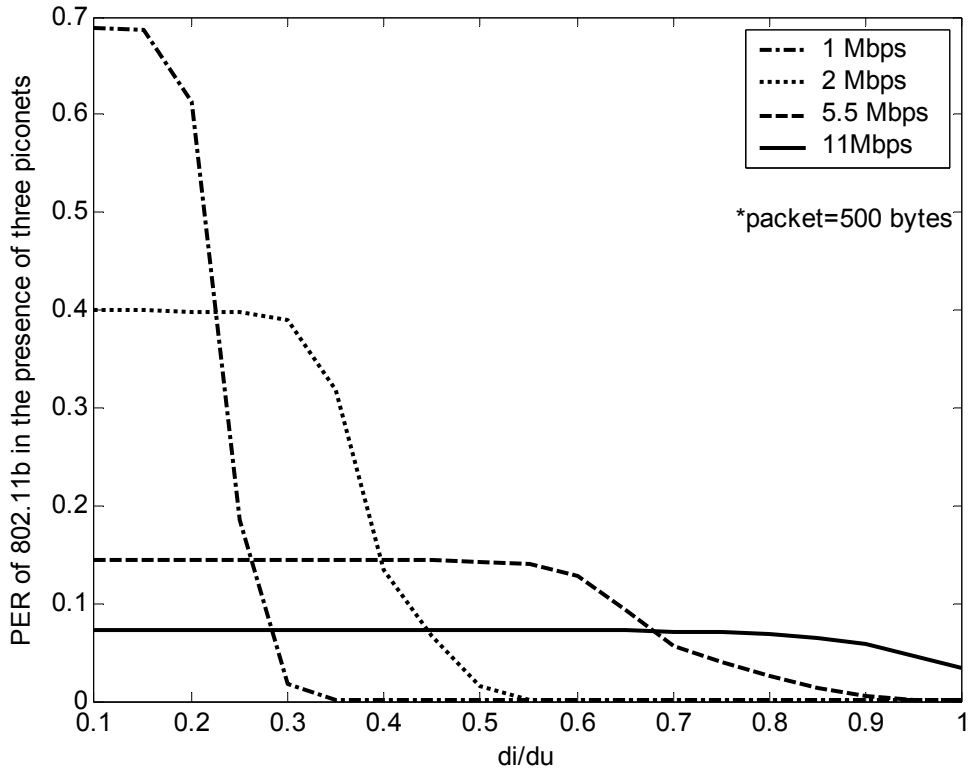

Figure 5.9 safe distance for an 802.11 receiver in the presence of three piconets

5.3.3 Packet Segmentation

Since there are four data rates defined within 802.11b, the temporal duration of the WLAN packets can vary significantly, for packets carrying the exact same data. The longer the duration of the WLAN packet, the more likely it will collide with an interfering Bluetooth packet, and the more likely that it may be destroyed if the interference is really strong. In case this happens, the transmitter resends the same packet several times before it successfully reaches the receiver. This would take much more time than sending a smaller packet. By reducing the size of the packets transmitted, there is a better probability of successful transmission. Therefore, packet segmentation is a potential strategy under poor channel conditions [9]. In general, however, a long packet could increase system throughput. Under good channel

conditions, segmentation is a hindrance because the associated overhead tends to reduce the aggregate throughput. Packet segmentation is allowed in the IEEE 802.11b standard at the MAC layer; so that the segment size could vary from 100 to 2350 bytes. One way to optimize the total throughput of the system is to optimize the throughput at each of the data rates. Consequently, we propose a packet segmentation scheme that is based on adapting the packet size at each data rate.

Recall the 802.11b segmentation mechanisms: the data within a large packet is broken into a sequence of smaller packets. This yields a sequence of DATA frames and corresponding Acknowledgement (ACK) frames that are exchanged with only a short interval, Short Inter Frame Space (SIFS) and Distributed Inter Frame Space (DIFS), separating the ACK and the subsequent DATA transmission, thus minimizing the probability that other transmitters might seize the medium. If a collision or other transmission impairment causes a DATA-ACK exchange to fail, the remaining sequence of segments is continued as before when the transmitter is able to successfully re-seize the medium [9]. For simplicity, we assume that the transmitter can re-seize the medium at average backoff contention time of $\overline{T}_{backoff} = \frac{CW_{\min}}{2} \cdot aSlotTime$ [31].

Suppose two 802.11b stations, one working as transmitter and the other as receiver, are operating in the range of significant interference from Bluetooth. Let us see what the best packet segmentation size is for different data rates. Figure 5.10 shows the throughput performance of an 802.11b receiver as a function of packet duration. Three curves present different interference scenarios, impacted by one, two and three piconets respectively. The maximum throughput is found at 2192 μs for the receiver in the presence of one piconet. By deducting overhead duration of 192 μs, it

corresponds to the optimum packet size of 250 bytes for 1 Mbps; 500 bytes for 2 Mbps; and so on. Observing the maximum throughput in the presence of two and three piconets, the optimum packet sizes of 167 and 129 bytes are obtained. Table 5.6 summarizes the optimum packet sizes for 802.11b four data rates operating within dangerous distance ranges. By using the suggested optimum packet sizes at each data rate, the transmitter could reach its maximum throughput at that rate.

Table 5.6 the optimum packet size for 802.11b in the presence of Bluetooth

Data rates / Conditions	1 Mbps (bytes)	2 Mbps (bytes)	5.5 Mbps (bytes)	11 Mbps (bytes)
Piconets = 1	(2192-192)/8	500	1375	2750
Piconets = 2	(1528-192)/8	334	918	1837
Piconets = 3	(1224-192)/8	258	709	1419

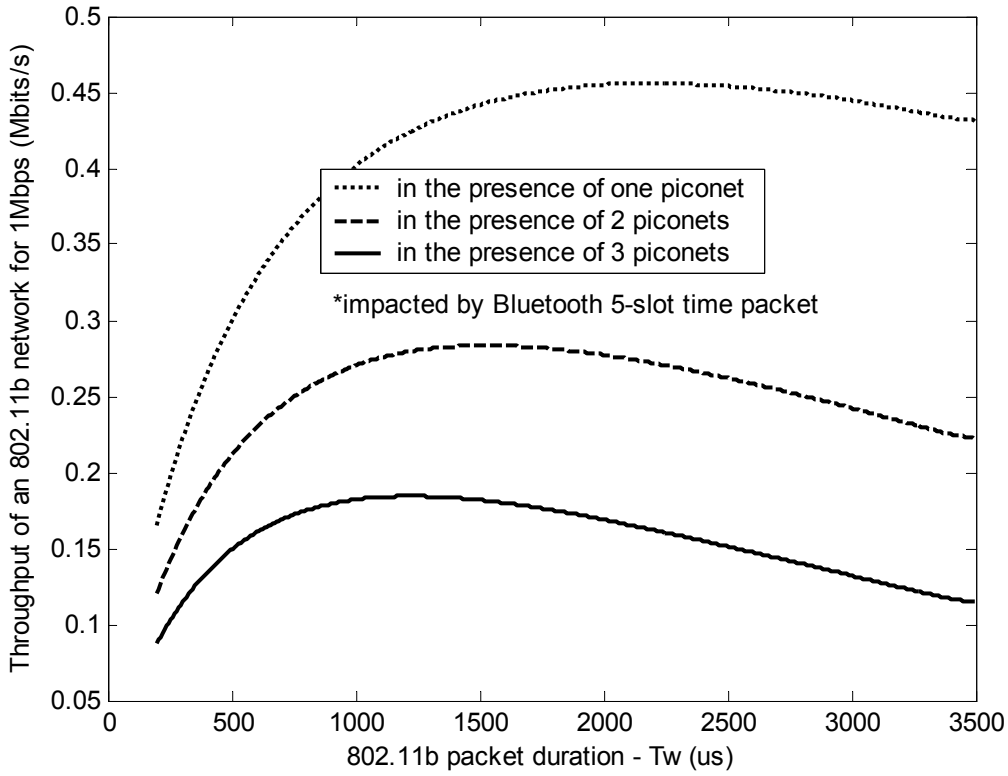

Figure 5.10 Throughput of an 802.11b network in the presence of Bluetooth

We know from those distance ratio graphs that there exist two kinds of operation range, safe distance and dangerous distance. In the safe distance range, the system should select the segmentation size of 2350 bytes, which is the longest one the MAC layer allowed; in the dangerous distance range, the packet segmentation sizes should be selected according to the results we get in Table 5.6. The safe and dangerous distance ratios are given in Table 5.5. Thus we obtain the optimum packet sizes for each rate as a function of the distance ratio d_i / d_u and the number of piconets, which is listed in Table 5.7. Note that the optimum segmentation size given here is to ensure the corresponding data rate achieve its maximum throughput under current link, but not ensure the data rate is the most efficient to other data rates. Research on data rate scaling for optimal throughput under certain link will be discussed in next subsection.

Table 5.7 The optimum packet sizes for each data rate

	piconets=1				piconets=2				piconets=3			
	11	5.5	2	1	11	5.5	2	1	11	5.5	2	1
1.0	2350	2350	2350	2350	1837	2350	2350	2350	1419	2350	2350	2350
0.9	2350	2350	2350	2350	1837	2350	2350	2350	1419	2350	2350	2350
0.8	2350	2350	2350	2350	1837	918	2350	2350	1419	709	2350	2350
0.7	2350	1375	2350	2350	1837	918	2350	2350	1419	709	2350	2350
0.6	2350	1375	2350	2350	1837	918	2350	2350	1419	709	2350	2350
0.5	2350	1375	2350	2350	1837	918	2350	2350	1419	709	258	2350
0.4	2350	1375	500	2350	1837	918	334	2350	1419	709	258	2350
0.3	2350	1375	500	2350	1837	918	334	2350	1419	709	258	129
0.2	2350	1375	500	250	1837	918	334	167	1419	709	258	129
0.1	2350	1375	500	250	1837	918	334	167	1419	709	258	129

5.3.4 Data Rate Scaling

The MAC layer is where data rates are determined, so this is the place to resolve data rate versus packet size trade-offs. It is possible for the Bluetooth interference to cause the WLAN to scale to a lower data rate [78]. At a lower data rate the duration of the WLAN is increased. This increase in packet duration can lead to increase in packet collisions with the interfering Bluetooth packets. In some implementations, this can lead to yet a further decrease in the WLAN data rate. To solve this problem we should know the maximum throughput for each data rate in different interference conditions. We have discussed the efficiency of each rate versus distance in interference free environment. Then we discussed the safe distance ratio for the WLAN in the presence of Bluetooth. We know the maximum segment size is 2350 bytes allowed in the IEEE 802.11b at MAC layer. Thus the WLAN should use the packet size as long as 2350 bytes when the WLAN is operating in safe distance range or interference free environment. Then we discuss the optimum packet sizes for each data rate when the WLAN is operating in dangerous distance range to Bluetooth, and we know the sizes are varying according to the number of interferers.

By given the packet size and distance, we can compute corresponding PER for the optimum packet segmentation sizes listed in Table 5.7. It is recorded in Table 5.8.

Table 5.8 The PER for each data rate corresponding to optimum packet size

	piconets=1				piconets=2				piconets=3			
	11	5.5	2	1	11	5.5	2	1	11	5.5	2	1
1.0	0.38	0.0	0.0	0.0	0.59	0.0008	0.0	0.0	0.71	0.009	0.0	0.0
0.9	0.38	0.0	0.0	0.0	0.59	0.018	0.0	0.0	0.71	0.06	0.0	0.0
0.8	0.38	0.005	0.0	0.0	0.59	0.08	0.0	0.0	0.71	0.71	0.0	0.0
0.7	0.38	0.136	0.0	0.0	0.59	0.59	0.0	0.0	0.71	0.71	0.0	0.0
0.6	0.38	0.40	0.0	0.0	0.59	0.59	0.0	0.0	0.71	0.71	0.0	0.0
0.5	0.38	0.40	0.0	0.0	0.59	0.59	0.02	0.0	0.71	0.71	0.088	0.0
0.4	0.38	0.40	0.1	0.0	0.59	0.59	0.59	0.0	0.71	0.71	0.71	0.0
0.3	0.38	0.40	0.40	0.0	0.59	0.59	0.59	0.01	0.71	0.71	0.71	0.087
0.2	0.38	0.40	0.40	0.40	0.59	0.59	0.59	0.59	0.71	0.71	0.71	0.71
0.1	0.38	0.40	0.40	0.40	0.59	0.59	0.59	0.59	0.71	0.71	0.71	0.71

Table 5.9 Data rate scaling algorithm

	piconets=1				piconets=2				piconets=3			
	11	5.5	2	1	11	5.5	2	1	11	5.5	2	1
1.0	4.49	4.38	1.83	0.95	**2.73**	**4.38**	1.83	0.95	**1.71**	**4.34**	1.83	0.95
0.9	4.49	4.38	1.83	0.95	**2.73**	**4.3**	1.83	0.95	**1.71**	**4.12**	1.83	0.95
0.8	4.49	4.36	1.83	0.95	**2.73**	**3.06**	1.83	0.95	1.71	**0.85**	**1.83**	0.95
0.7	4.49	3.3	1.83	0.95	2.73	**1.36**	**1.83**	0.95	1.71	**0.85**	**1.83**	0.95
0.6	4.49	2.29	1.83	0.95	2.73	**1.36**	**1.83**	0.95	1.71	**0.85**	**1.83**	0.95
0.5	4.49	2.29	1.83	0.95	2.73	**1.36**	**1.79**	0.95	1.71	**0.85**	**0.99**	0.95
0.4	4.49	2.29	1.25	0.95	2.73	1.36	**0.5**	**0.95**	1.71	0.85	**0.31**	**0.95**
0.3	4.49	2.29	**0.83**	**0.95**	2.73	1.36	**0.5**	**0.86**	1.71	0.85	**0.31**	**0.49**
0.2	4.49	2.29	0.83	0.42	2.73	1.36	0.5	0.25	1.71	0.85	0.31	0.16
0.1	4.49	2.29	0.83	0.42	2.73	1.36	0.5	0.25	1.71	0.85	0.31	0.16

The maximum throughput (Mbits/s) of each rate in different interference conditions, therefore, is obtained via computation of Table 5.7 and 5.8, and recorded in Table 5.9.

We mark those points which the maximum throughput is smaller than that of the lower rate with shading. The points also indicate the data rate scaling boundaries. We can see if there is only one piconet, 11 Mbps performs best for all the ratios. It is also observed the 1 Mbps outperforms the 2 Mbps when $d_i / d_u = 0.3$. When Bluetooth piconets increase to two, we have to abandon the use of 11 Mbps; and 5.5 Mbps outperforms at the ratios of 0.8 to 1.0; then have to scale to 2 Mbps if ratios decrease to 0.7; if interferer is much closer to the ratio of 0.4, scaling to 1 Mbps is best for the system. Similar observation can be got when piconets increase to three.

5.4 Effects of Traffic Load

For this topic we just discuss the effects of a simple traffic load change on the systems. Up to now, we always assume full traffic load in Bluetooth and 802.11b network. It is the worst case for the systems because there is no time slot that the interferer will be off. A simple traffic load scheme is to reduce the transmitting packets in the channel. This is equivalent to reducing the number of interferers in the proximity. An example of full load is a Bluetooth SCO link of 2-slot period, which occupies the whole capacity of a piconet. If it is changed to 4-slot period, the traffic load is reduced to half. If an 802.11b system coexists with two closed Bluetooth piconets, this traffic load change is equal to the number of interferers to be reduced from two to only one. So the effect of traffic load can be approximated as a linear relationship with the number of interferers; the proportion of traffic load reduction means the number of interferers reduction.

CHAPTER 6

CONCLUSIONS AND FUTURE WORK

6.1 Conclusions

The objective of the research disclosed in this thesis was to develop a model for a complete analytical study for the mutual interference between two systems by means of an integrated approach, which properly takes all transmission aspects (propagation effects, interference, thermal noise, modulations, coding techniques, data rates) and medium access control aspects (frequency hopping, packet structure, packet size adjustment, traffic load) into account. This study then leads the research on how to optimize system throughput in a situation with numerous, disparate, and uncoordinated interferers.

In the BER analysis part, the error probability of CCK is derived. Results show that CCK modulation technique is better than DPSK modulation. At the same E_b / N_0 ratio, CCK 11Mbps outperforms CCK 5.5 Mbps, DBPSK and DQPSK. In the 802.11b system, the transmit power is kept fixed for each data rate, thus as a result, 1 Mbps performs best, followed by 2 Mbps, 5.5 Mbps and 11 Mbps, at the same E_S / N_0. The efficient operating distance of higher rates is shorter than that of the lower rates.

In the collision analysis part, the mutual interference between Bluetooth and Bluetooth, Bluetooth and 802.11b, and conversely, 802.11b and Bluetooth, are evaluated. For the interference between Bluetooth and Bluetooth, we find there are different numbers of co-worked competitors that a Bluetooth piconet can tolerate depending on each packet

type used. For the piconet using 1-slot packet, it can tolerate 7 piconets, where they all make use of 1-slot packet type; or 8 piconets if they make use of 3 or 5-slot types. Considering fairness among all the coexisting piconets, the same packet type should be used in each piconet. Thus we can see 1-slot packet type is suitable for each piconet in high density interference environment, up to 8 piconets; 3-slot type suits to less than 6 piconets; while 5-slot type is used when less than 4 piconets.

It is observed that the interference from 802.11b on Bluetooth is in form of frequency static interference because they are always from a fixed frequency band. From the result, we find the collision probability of 1-slot packet type correlates with 802.11 packet length because we assume it is shorter than $T_{backoff}$. But for 3 or 5-slot time packet, it is a constant collision probability because their length is longer than $T_{backoff}$.

The reciprocal scenario where the effect of Bluetooth piconets on 802.11b is considered. We find 802.11b packet suffers the most from Bluetooth 1-slot packet type, then 3 and 5-slot types. Since the use of multiple time slot packets effectively reduces the Bluetooth hop rate, thereby increasing the chances of successful reception of WLAN packets.

In Chapter 4, a more accurate and practical model is proposed in the evaluation of PER by combining both PHY and MAC layers. By taking the distance effects into account, smaller PERs are obtained than using collision probability. And the results of PER are suitable for a more realistic scenario.

The study on mutual interference between the two systems gives us some insight of how the systems work in a particular scenario. In Chapter 5, we try to figure out how to enhance systems' performance by selecting the optimum packet type, packet size, safe distance, data speed, and etc. For Bluetooth system, the optimum packet types for

a Bluetooth device in the presence of multiple piconets are found by using throughput calculation. They are summarized in Table 5.3. Considering fairness among the piconets, each piconet should use same packet types. Thus the results show that the throughput of 1-slot packet type outperforms other types when the number of interference reaches to 15; for 3-slot type, it is above 7; while 5-slot type could always maintain the highest throughput if interferers are less than 12. The long packet type is also suggested to use in the presence of 802.11b.

For the reciprocal scenario that 802.11b affected by Bluetooth, the efficient operating range for each data rate is obtained. 11 Mbps gives best throughput for the first 50 meters, then 5.5 Mbps performs the best for the next 15 meters, then 2 Mbps becomes more efficient for next 20 meters and finally 1Mbps gives the best throughput at 80 meters and beyond. Through the PER calculation, we find the safe distance range for an 802.11b receiver from Bluetooth interference. Thus when the WLAN is operating in safe distance range or interference free environment, the long segmentation size of 2350 bytes is suggested to use. Then the optimum packet sizes are found for each data rate under significant interference from Bluetooth. The proper moment for data rate scaling of the system under significant interference is also discussed carefully. We find 11 Mbps has the maximum throughput in the presence of one Bluetooth piconet. When piconets increase, 11 Mbps mode has to be abandoned, and data rate scaling can take place at the proper distance ratio.

To sum up, by using the proposed evaluation framework, the impact of interference where two systems are affecting each other is easily obtained. But it must be emphasized that the results of this analysis should be considered preliminary. It should be stressed that interference between radio systems is highly variable and depends on a number of factors, primarily geometry of the nodes. Given the nature of radio-wave

propagation and implementation limitations of receiver design, it is always possible to construct scenarios that will give pathologically poor performance (or unrealistically excellent performance). The conclusions represent neither extreme, but are indicative of the results that led the industry to look for solutions.

6.2 Future work

6.2.1 ISI and Frequency Selective

In this thesis, we ignore the effect of inter-symbol interference (ISI). Actually, in the indoor environment, signals can arrive at the antenna by more than one path. In addition, the distance of each path can be quite different. Each signal path from the transmitter to the receiver has a unique time delay and phase shift associated with it. For this reason, the received signal can be severely distorted. Some frequencies within the signal bandwidth combine constructively, increasing signal strength. Others combine destructively, thereby reducing signal strengths at that particular frequency. This phenomenon is called frequency selective. In the indoor environment, energy reaching the receiver antenna via delayed paths can spill from one symbol into subsequent symbols. In fact, some secondary paths can have delays equivalent to several symbol times. IEEE 802.11b devices employ a waveform known CCK. The underlying modulation is single-carrier QPSK. At 11 Mbps, a symbol period is about 91 ns. However, some secondary paths have delays of 400 to 500 ns. In these situations, ISI can result in distortion of as many as five or six subsequent symbols. Consequently, energy transmitted in one symbol period can distort several subsequent symbols. Thus, multipath can cause ISI resulting in several signal distortion.

6.2.2 Experimental Measurements Studies

Published results can be classified into at least three categories depending on whether they rely on analysis, simulation, or experimental measurements. Analytical results based on probability of packet collision were obtained in this thesis. Although these analytical results can often give a first order approximation on the impact of interference and the resulting performance degradation, they often make a number of assumptions such as the channel model, the interference model and the radio propagation model, which can make them less realistic. On the other hand, experimental results are highly site-specific and can be considered more accurate at the cost of being too specific to the implementation tested. So the approach of analysis combined with experimental measurements is a highly useful tool for predicting performance that can be tied to average measurements.

6.2.3 Other New Technologies in the 2.4 GHz ISM Band

In November 2001 the IEEE 802.11 committee adopted a draft standard called 802.11g that will provide data rates of up to 54 Mbps in the 2.4 GHz band using Orthogonal Frequency Division Multiplexing (OFDM) as the physical layer modulation format [79]. 802.11g systems are still in their infancy. The proposed OFDM technology is originally used in the 802.11a standard in the 5 GHz band. But now as the restriction of prohibiting the use of OFDM in the 2.4 GHz band was lifted in May of 2001 [80], it is reused in the 2.4 GHz. Though the MAC specification has remained largely unchanged until now (except for Quality of Service (QoS) enhancements under 802.11e [81]), the 802.11g physical layer is based on the use of OFDM which is arguably the best waveform available today for WLAN applications. OFDM for

802.11g splits an information signal across 52 separate subcarriers to provide transmission of data at a rate of 6, 9, 12, 18, 24, 36, 48 or 54 Mbps. Four of the subcarriers are pilot subcarriers that the system uses as a reference to disregard frequency or phase shifts of the signal during transmission. The remaining 48 subcarriers provide separate wireless pathways for sending the information in a parallel fashion. Various combinations of coding rate and modulation scheme are specified in order to facilitate different modes of transmission [82]. These different modes are defined in Table 6.1. OFDM was developed specifically for indoor wireless use and offers performance much superior to that of DSSS solutions. OFDM works by breaking one high speed data carrier into several lower speed subcarriers. Each subchannel in the OFDM implementation is about 300 KHz wide. This enables a significantly longer symbol period. For BPSK in 802.11g 6 Mbps mode, the data rate in each subchannel is 125 Kbps. A symbol period is about 8000 ns, which is much longer than path delays in an indoor environment.

Table 6.1 Modulation Techniques employed by 802.11g

Data Rate (Mbps)	Modulation	Coding Rate	Coded bits per subcarrier	Coded bits per OFDM symbol	Data bits per OFDM symbol
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	16-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

In OFDM the subcarrier pulse used for transmission is chosen to be rectangular. In the frequency-domain, the rectangular pulse is represented by a *sin(x)/x* type of spectrum with zero-crossings at intervals corresponding to the inverse of the pulse period. At the zero crossing, there is no energy from adjacent subcarriers. Subcarriers are

therefore said to be “orthogonal” [83][84]. According to the frequency-domain the orthogonal subcarriers of OFDM is shown in Figure 6.1. Obviously the spectrums of the subcarriers are not separated but overlay. Each stream is then mapped to a subchannel and combined together using an *Inverse Fast Fourier Transform* (IFFT) to yield the time-domain waveform to be transmitted. The receiver samples at the center frequency of each subchannel, the only energy present is that of the desired signal. Even though the OFDM subcarriers are very closely spaced, they do not interfere with each other.

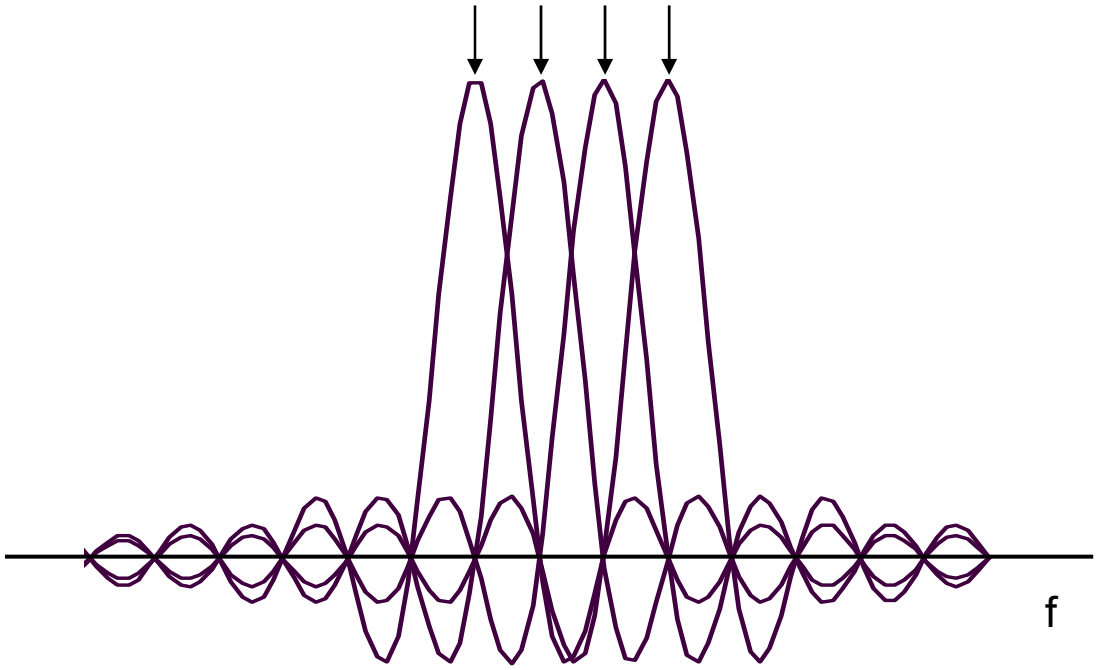

Figure 6.1 OFDM and the orthogonal principle

Even though the PHY is the same in both 5 GHz and 2.4 GHz, the actual operating environment is very different in the 2.4 GHz band and hence implementations developed for 5 GHz if used directly at 2.4 GHz will cause system degradation. One of the main impediments in WLAN system performance in the 2.4 GHz band is the presence of Bluetooth system in the same band. Some work has been performed in

[85]-[88]. In [85], the effect of Bluetooth interference on OFDM-based WLAN is evaluated. The BER performance of OFDM on BPSK modulation is obtained by an average for all N subcarriers. The intense performance degradation of uncoded OFDM system is found under Bluetooth environments. A coded OFDM-based WLAN, however, can effectively mitigate Bluetooth interference through coding and interleaving even at a low SIR. The optimum operating coverage for different data rate modes is studied in the presence of Bluetooth interference in [86]. The impact of Bluetooth interference on the 802.11g is investigated more carefully in [87] and [88] by considering the relative power levels of the interferers, packet lengths as well as the influence of FEC schemes used in the packets are considered. Then in the paper of [79], a PHY layer algorithm that can cancel Bluetooth interference is presented. Anyway, the research on the coexistence of Bluetooth and 802.11g or 802.11b and 802.11g is just beginning. The eight available data rate modes defined in 802.11g have not been studied thoroughly. With growingly demanding utilization of the free and unlicensed 2.4 GHz band, the coexistence issue among different technologies will attract more and more research on it.

REFERENCES

[1] S. Zurbes, W. Stahl, K. Matheus and J. Haartsen, "Radio network performance of Bluetooth", Proc. of IEEE Int. Conf. on Communications, vol. 3, pp. 1563-1567, Jun. 2000.

[2] S. Souissi, E.F. Meihofer, "Performance evaluation of a Bluetooth network in the presence of adjacent and co-channel interference", Emerging Technologies Symposium: Broadband, Wireless Internet Access, IEEE, 10-11 April 2000.

[3] A. El-Hoiydi, "Interference between Bluetooth networks – upper bound on the packet error rate", IEEE communications letters, vol. 5, No. 6, Jun. 2001.

[4] F. Mazzenga, D. Cassioli, P. Loreti and F. Vatalaro, "Evaluation of packet loss probability in Bluetooth networks", IEEE Int. Conf. on Communications, vol. 1, pp. 313-317, May 2002.

[5] T.Y. Lin and Y.C. Tseng, "Collision analysis for a multi-Bluetooth picocells environment", IEEE communications letters, vol. 7, No. 10, Oct. 2003.

[6] N. Golmie and F. Mouveaux, "Interference in the 2.4 GHz ISM band: impact on the Bluetooth access control performance", Communications, IEEE International Conference on , Vol. 8, Pages:2540 – 2545, June 2001.

[7] J. Lansford, R. Newo, and B. Monello, "Wi-Fi (802.11b) and Bluetooth simultaneous operation: characterizing the problem", in Mobilian White Paper, www.mobilian.com, Sept. 2000.

[8] I. Howitt, "Bluetooth performance in the presence of 802.11b WLAN", IEEE trans. on vehicular technology, vol. 51, No. 6, Nov. 2002.

[9] G. Ennis, "Impact of Bluetooth on 802.11 direct sequence", IEEE Doc: IEEE P802.11-98/319.

[10] J. Zyren, "Extension of Bluetooth and 802.11 direct sequence interference model", IEEE Doc: IEEE P802.11-98/378, Nov. 1998.

[11] S. Shellhammer, "Packet error rate of an IEEE 802.11 WLAN in the presence of Bluetooth", IEEE Doc: IEEE 802.15-00/133r0, May 2000.

[12] C.F. Chiasserini and R.R. Rao, "Performance of IEEE 802.11 WLANs in a Bluetooth environment", IEEE wireless communication and networking conference, vol. 1, pp. 94-99, Sept. 2000.

[13] I. Howitt, "IEEE 802.11 and Bluetooth coexistence analysis methodology", Vehicular Technology Conference, VTC 2001 Spring. IEEE VTS 53rd , Volume: 2 , pp. 1114 – 1118, May 2001.

[14] I. Howitt, “WLAN and WPAN coexistence in UL band”, IEEE trans. on vehicular technology, vol. 50, No. 4, pp. 1114-1124, July 2001.

[15] G. Pasolini, “Bluetooth piconets coexistence: analytical investigation on the optimal operating conditions”, Communications, 2003. ICC '03. IEEE International Conference on, Volume: 1, pp. 198-202, May 2003.

[16] B. Jiang and O. Yang, “Performance evaluation of Bluetooth system in the presence of WLAN IEEE 802.11 system”, Electrical and Computer Engineering, 2003. IEEE CCECE 2003. Canadian Conference on , Volume: 3 , pp. 1633-1636, May 2003.

[17] M. Fainberg and D. Goodman, “Analysis of the interference between IEEE 802.11b and Bluetooth systems”, Vehicular Technology Conference, VTC 2001 Fall. IEEE VTS 54th , Volume: 2, pp. 967-971, Oct. 2001.

[18] N. Golmie, R.E. Van Dyck and A. Soltanian, “Interference of Bluetooth and IEEE 802.11: simulation modeling and performance evaluation”, Proceedings of the 4th ACM international workshop on modeling, analysis and simulation of wireless and mobile systems, Rome, Italy, Jul. 2001.

[19] N. Golmie, R.E. Van Dyck, A. Soltanian, A. Tonnerre and O. Rebala, “Interference evaluation of Bluetooth and IEEE 802.11b systems”, Wireless Networks 9, Kluwer Academic Publishers, pp. 201-211, 2003.

[20] A. Conti, D. Dardari, G. Pasolini and O. Andrisano, “Bluetooth performance analysis under IEEE 802.11 interference in a fading channel”, Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE , Volume: 1, pp. 227-232, Nov. 2002.

[21] A. Conti, D. Dardari, G. Pasolini and O. Andrisano, “Bluetooth and IEEE 802.11b coexistence: analytical performance evaluation in fading channels”, IEEE journal on selected areas in communications, vol. 21, No. 2, Feb. 2003.

[22] O. Andrisano, A. Conti, D. Dardari, B.M. Masini and G. Pasolini, “Bluetooth and IEEE 802.11 coexistence: analytical performance evaluation in fading channel”, Personal, Indoor and Mobile Radio Communications, 2002. The 13th IEEE International Symposium on, Volume: 4, pp. 1752-1756, Sept. 2002.

[23] J. Zyren, “Reliability of IEEE 802.11 WLANs in presence of Bluetooth radios”, IEEE Doc: IEEE 802.15-99/073r0, Sept. 1999.

[24] J.H. Jo and N. Jayant, “Performance evaluation of multiple IEEE 802.11b WLAN stations in the presence of Bluetooth radio interference”, IEEE International Conference on Communications, vol. 26, no. 1, pp. 1163-1168, May 2003.

[25] A. Kamerman, “Coexistence between Bluetooth and IEEE 802.11 CCK solutions to avoid mutual interference”, Lucent Technologies Bell Laboratories, Jan. 1999.

[26] C.F. Chiasserini and R.R. Rao, “A comparison between collaborative and non-collaborative coexistence mechanisms for interference mitigation in ISM bands”,

Vehicular Technology Conference, 2001. VTC 2001 Spring. IEEE VTS 53rd, vol. 3, pp. 2187-2191, May 2001.

[27] B. Zhen, Y. Kim and K. Jang, "The analysis of coexistence mechanisms of Bluetooth", Vehicular Technology Conference, 2002. VTC Spring 2002. IEEE 55th,Volume: 1, pp. 419 – 423, May 2002.

[28] M.V.S. Chandrashekhar, P. Choi, K. Maver, R. Sieber, "Evaluation of interference between IEEE 802.11b and Bluetooth in a typical office environment", Personal, Indoor and Mobile Radio Communications, 2001. 12th IEEE International Symposium on, vol. 1, pp. D71-D75, 2001.

[29] J. del Prado and S. Choi, "Experimental study on co-existence of 802.11b with alien devices", Vehicular Technology Conference, VTC 2001 Fall. IEEE VTS 54th,Vol. 2, pp. 977-981, Oct. 2001.

[30] S. Zurbes, "Considerations on link and system throughput of Bluetooth networks", Personal, Indoor and Mobile Radio Communications, 2000. PIMRC 2000. The 11th IEEE International Symposium on, Volume: 2, pp. 1315-1319, Sept. 2000.

[31] J. del Prado and S. Choi, "Link adaptation strategy for IEEE 802.11 WLAN via received signal strength measurement", Communications, 2003. ICC '03. IEEE International Conference on,Vol. 2, pp. 1108-1113, May 2003.

[32] M.C. Valenti and M. Robert, "Custom coding, adaptive rate control, and distributed detection for Bluetooth", Vehicular Technology Conference, 2002. Proceedings. VTC 2002-Fall. 2002 IEEE 56th,Volume: 2, pp. 918-922, Sept. 2002.

[33] C.F. Chiasserini and R.R. Rao, "Coexistence mechanisms for interference mitigation in the 2.4 GHz ISM band", IEEE trans. on wireless communications, vol. 2, No. 5, pp. 964-975, Sept. 2003.

[34] W.T. Chen, B.B. Jian and S.C. Lo, "An adaptive retransmission scheme with QoS support for the IEEE 802.11 MAC enhancement", Vehicular Technology Conference, 2002. VTC Spring 2002. IEEE 55th , Volume: 1, pp. 70-74, May 2002.

[35] A. Soltanian, R.E. Van Dyck and O. Rebala, "Rejection of Bluetooth interference in 802.11 WLANs", Vehicular Technology Conference, 2002. Proceedings. VTC 2002-Fall. 2002 IEEE 56th,Volume: 2, pp. 932-936, Sept. 2002.

[36] K. Kim and G.L. Stuber, "Interference mitigation in asynchronous slow frequency hopping Bluetooth networks", Wireless personal communications 28, Kluwer Academic Publishers, pp. 143-159, 2004.

[37] Y.I. Joo, J.S. Oh, O.S. Kwon, Y. Kim, T.J. Lee and K.H. Tchah, "An efficient and QoS-aware scheduling policy for Bluetooth", Vehicular Technology Conference, 2002. Proceedings. VTC 2002-Fall. 2002 IEEE 56th, Volume: 4, pp. 2445-2448, Sept. 2002.

[38] A. Soltanian and R. E. Van Dyck, "Physical layer performance for coexistence of Bluetooth and EEE802.11b," presented at the Virginia Tech. Symp.Wireless Personal Communications, Blacksburg, VA, June 2001

[39] M. Shimizu, N. Aoki, K. Shirakawa, Y. Tozawa, N. Okubo, Y. Daido, "New method of analyzing BER performance of GFSK with postdetection filtering", Communications, IEEE Transactions on , Volume: 45 , Issue: 4 , Pages:429 – 436, April 1997.

[40] M.C. Valenti, M. Robert, J.H. Reed, "On the throughput of Bluetooth data transmissions", IEEE Wireless Communications and Networking Conference, Vol. 1 , Pages:119 – 123, March 2002.

[41] J. G. Proakis, "Digital communications", 4th edition, McGraw-Hill, 2000.

[42] G.J.M. Janssen, P.A. Stigter and R. Prasad, "Wideband indoor channel measurements and BER analysis of frequency selective multipath channels at 2.4, 4.75 and 11.5 GHz", IEEE transactions on communications, Vol. 44, No. 10, pp. 1272-1288, Oct. 1996.

[43] S. C. Kim, H. L. Bertoni, and M. Stern, "Pulse propagation characteristics at 2.4 GHz inside buildings," IEEE Trans. Veh. Technol., vol. 45, pp. 579–592, Aug. 1996.

[44] Y.P. Zhang and Y. Hwang, "Time delay characteristics of 2.4 GHz band radio propagation channels in room environments", Personal, Indoor and Mobile Radio Communications, 5th IEEE International Symposium on,Vol. 1, pp. 28 – 32, Sept. 1994.

[45] H.J. Zepernick and T.A. Wysocki, "Multipath channel parameters for the indoor radio at 2.4 GHz ISM band", Vehicular Technology Conference, 1999 IEEE 49th ,Vol. 1, pp.190 – 193, May 1999.

[46] M.K. Simon and M.S. Alouini, "Digital communication over fading channels", 1st Ed. New York, Wiley, 2000.

[47] J.C. Haartsen and S. Mattisson, "Bluetooth – a new low-power radio interface providing short-range connectivity," Proceedings of the IEEE, Vol. 88, No. 10, pp. 1651-1661, Oct. 2000.

[48] "Specifications of the Bluetooth system", Vol. 1, version: 1.0B, Dec. 1999.

[49] A. Nallanathan, Course notes on "Digital communications", Dept. ECE, National University of Singapore, 2001.

[50] R. Steele, "Mobile radio communications", Hohn Wiley & Sons Inc., 1996.

[51] J. Sun, "Complementary Code Keying Modulation," http://www.csee.wvu.edu/~jian/article/cck.htm.

[52] M.K. Simon and C.C. Wang, “Differential detection of Gaussian MSK in a mobile radio environment”, IEEE Trans. Veh. Tech. pp 307-320, Nov. 1984.

[53] J. Chow and N. C. Beaulieu, “Analysis of cochannel interference in angle modulation Systems,” in Proc. IEEE Pacific Rim Conf Communications, Computers and Signal Processing, Victoria, Canada, pp. 123–127, Aug. 1999.

[54] J. Cheng, N.C. Beaulieu, “Error rate of BPSK in generalized fading channels with co-channel interference”, VTC Spring 2002. IEEE 55th, Volume: 4, Pages:1786 - 1790, May 2002.

[55] D. Dardari, G. Pasolini, “Simple and accurate models for error probability evaluation of IEEE802.11 DS-SS physical interface in the presence of Bluetooth interference”, Global Telecommunications Conference, IEEE, Volume: 1, Pages:201 – 206, Nov. 2002.

[56] IEEE Std. 802-11, “IEEE standard for Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specification”, 2001 edition.

[57] B.P. Crow, I. Widjaja, J.G. Kim and P.T. Sakai, “IEEE 802.11 wireless local area networks”, IEEE Communications Magazine, pp. 116-126, Sept. 1997.

[58] C. Andren and M. Webster, “CCK Modulation Delivers 11 Mbps for High Rate IEEE 802.11 Extension,” Wireless Symp., Portable by Design Conference, Spring, 1999.

[59] C. Andren, M. Webster and K. Halford, “CCK, the new IEEE 802.11 standard for 2.4 GHz wireless LANs”, conference proceedings on international IC – Taipei.

[60] R.D.J. van Nee, “OFDM codes for peak-to-average power reduction and error correction”, GLOBECOM '96. Volume: 1, Pages:740 - 744, Nov. 1996.

[61] B. Pearson, “Complementary code keying made simple”, Application Note 9850, Intersil.

[62] J.G. Proakis and M. Salehi, “Contemporary communication systems using MATLAB”, Pacific Grove, CA: Brooks/cole, 2000.

[63] J. Lansford, A. Stephens and R. Nevo, “Wi-Fi (802.11b) and Bluetooth: enabling coexistence”, IEEE Network, Vol. 15, Issue 5, pp. 20-27, Sept.-Oct. 2001.

[64] IEEE P802.15 wireless local area networks. IEEE documentation, IEEE P802.15-01418r0.

[65] Theodore S. Rappaport, “Wireless communications, principles and practice”, Prentice hall, New Jersey, 1998.

[66] R.E. Ziemer, “An overview of modulation and coding for wireless communications”, Vehicular Technology Conference, IEEE 46th, Volume: 1, Pages:26 – 30, May 1996.

[67] O. Andrisano, G. Corazza, and G. Immovilli, "Adjacent channel and cochannel interferences in CPFSK systems with nonlinear transmitters and limiter-discriminator detection", IEEE Trans. on Comms, Vol. 36, No. 5, pp. 544-552, May 1988.

[68] M. Fainberg, "Performance analysis of the 802.11b local area network in the presence of Bluetooth personal area network", Master of Science Dissertation, Polytechnic University, 2001.

[69] D. Cypher. (2000, Mar.) "Coexistence, interoperability, and other terms", IEEE 802.15-99/134r1, IEEE P802.15 working group for WPANs.

[70] IEEE 802.15 WPAN Task Group 2 (TG2). www.ieee802.org/15/pub/TG2.html.

[71] S. Shellhammer, (2001, Mar.) "An alternative to the Bluetooth SCO link for operation in an interference environment", IEEE 802.15-01/145r1, IEEE P802.15 working group for WPANs.

[72] H. Gan and B. Treister, (2000, Nov.) "Adaptive frequency hopping implementation proposals for IEEE 802.15.1/2 WPAN", IEEE 802.15-00/367r0, IEEE P802.15 working group for WPANs.

[73] B. Treister (2001, July) "Adaptive frequency hopping", IEEE 802.15-01/366r1, IEEE P802.15 working group for WPANs.

[74] B. Treister, H.B. Gan, K.C. Chen, H.K. Chen, A. Batra, and O. Eliezer, (2001, May) "Components of the AFH mechanism", IEEE 802.15-01/252r0, IEEE P802.15 working group for WPANs.

[75] N. Golmie, (2001, July) "Non-collaborative MAC mechanisms", IEEE 802.15-01/316r0, IEEE P802.15 working group for WPANs.

[76] M.B. Shoemake, (2001, Jan.) "Proposal for power control for enhanced coexistence", IEEE 802.15-00/081r0, IEEE P802.15 working group for WPANs.

[77] B.H. Walke, "Mobile Radio Networks: Networking, Protocols and Traffic Performance," 2nd Edition, Wiley, 2001.

[78] S. Shellhammer, "Description of the interference problem", IEEE documentation, IEEE P802.15-01/314r0.

[79] M. Ghosh and V. Gaddam, "Bluetooth interference cancellation for 802.11g WLAN receivers", Communications, ICC '03. IEEE International Conference on ,Vol. 2, pp. 1169-1173, May 2003.

[80] J. Zyren, E. Enders and T. Edmondson, "802.11g starts answering WLAN range questions", http://www.commsdesign.com, Jan. 2003.

[81] S. Mangold, S. Choi, P. May, O. Klein, G. Hiertz, L. Stibor, "IEEE 802.11e wireless LAN for quality of service", Proc. European Wireless (EW' 2002), Feb. 2002.

[82] “IEEE 802.11g ERP WLAN in the 2.4 GHz band 1-54 Mbps”, http://www.vocal.com, © 2002 VOCAL Technologies, Ltd.

[83] M. Speth, “OFDM receivers for broadband transmission”, http://www.ert.rwth-aachen.de/Projekte/Theo/OFDM/www_ofdm.html.

[84] “OFDM for mobile data communications”, On-line Education, International Engineering Consortium, http://www.iec.org/online/tutorials/ofdm.

[85] J. Park, D. Kim C. Kang and D. Hong, “Effect of Bluetooth interference on OFDM-based WLAN”, Vehicular Technology Conference, IEEE 58th VTC 2003-Fall., Vol. 2, pp. 786 – 789, Oct. 2003.

[86] K.K. Wong and T. O’Farrell, “Coverage of 802.11g WLANs in the presence of Bluetooth interference”, Personal, Indoor and Mobile Radio Communications, PIMRC 2003. 14th IEEE Proceedings on , Vol. 3, pp. 2027-2031, Sept. 2003.

[87] A. Doufexi, A. Arumugam, S. Armour and A. Nix, “An investigation of the impact of Bluetooth interference on the performance of 802.11g wireless local area networks”, Vehicular Technology Conference, the 57th IEEE Semiannual VTC 2003-Spring, Vol. 1, pp. 680-684, April 2003.

[88] A.K. Arumugam, A. Doufexi, A.R. Nix and P.N. Fletcher, “An investigation of the coexistence of 802.11g WLAN and high data rate Bluetooth enabled consumer electronic devices in indoor home and office environments”, Consumer Electronics, IEEE Transactions on ,Vol. 49, Issue: 3, pp. 587 – 596, Aug. 2003.

[89] N. Golmie, N. Chevrollier and I. ElBakkouri, “Interference aware Bluetooth packet scheduling”, Global Telecommunications Conference, IEEE, GLOBECOM '01,vol. 5, pp. 2857-2863, Nov. 2001.

LIST OF PUBLICATIONS

1. Wang Feng, A. Nallanathan and H. K. Garg, “Performance of a Bluetooth Piconet in the Presence of IEEE 802.11 WLAN”, Personal, Indoor and Mobile Radio Communications, PIMRC’02, vol. 4, Pages:1742 – 1746, Sept. 2002.

2. Wang Feng, A. Nallanathan and H. K. Garg, “Impact of Interference on a Bluetooth Network in the 2.4 GHz ISM Band”, Communication Systems, The 8th International Conference on , ICCS 2002, vol. 2, Pages:820 – 823, Nov. 2002.

3. Wang Feng, A. Nallanathan and H. K. Garg, “Imapct of Interference on the Performance of a Bluetooth Piconet in the 2.4 GHz ISM Band”, ELECTRONICS LETTERS, vol.38, no. 25, pp. 1721-1723, Dec. 2002.

4. Wang Feng, A.Nallanathan and H.K.Garg, " Performance of Physical (PHY) and Medium Access Control (MAC) Layers of IEEE 802.11b in the presence of Bluetooth Piconets " Proc of VTC 2003-Spring. vol. 2, Pages:1489 – 1492, April 2003.

5. Wang Feng, A. Nallanathan and H.K.Garg, "Introducing Packet Segmentation for the IEEE 802.11 Throughput enhancement in the Presence of Bluetooth " Proc. of IEEE VTC'S04, Italy, May 2004.

6. Wang Feng, A. Nallanathan and H.K. Garg, “Performance of PHY and MAC Layers of a Bluetooth Piconet in Multi-Bluetooth Interference Environment”, to appear in Proc of GLOBECOM 2004, Dallas, Texas USA.

7. Wang Feng, A. Nallanathan and H.K. Garg, “Performance Analysis of IEEE 802.11b WLAN in Fading Channels and Interference from Bluetooth”, Submitted to IEEE Transactions on Vehicular Technology.

8. Wang Feng, A. Nallanathan and H.K. Garg, “Co-existence of Bluetooth and IEEE 802.11b in Mutual Interference Environment: An Integrated Analysis”, submitted to IEE Proceedings, Communications.